Preprint of paper: final version appears as: ADAMS, A. & BLANDFORD, A. (2005) Bridging the gap between Organisational and User perspectives of security in the clinical domain. *International Journal of Human–Computer Studies*. 63. 175 - 202.

Bridging the gap between organisational and user perspectives of security in the clinical domain

Anne Adams (corresponding author)

Ann Blandford

UCL Interaction Centre, University College London, 31-32 Alfred Place, London, WC1E 7DP, UK
e-mail: a.adams@cs.ucl.ac.uk, a.blandford@cs.ucl.ac.uk

Abstract:

An understanding of 'communities of practice' can help to make sense of existing security and privacy issues within organisations; the same understanding can be used proactively to help bridge the gap between organisational and end-user perspectives on these matters. Findings from two studies within the health domain reveal contrasting perspectives on the 'enemy within' approach to organisational security. Ethnographic evaluations involving in-depth interviews, focus groups and observations with 93 participants (clinical staff, managers, library staff and IT department members) were conducted in two hospitals. All of the data was analysed using the social science methodology 'grounded theory'. In one hospital, a community and user-centred approach to the development of an organisational privacy and security application produced a new communication medium that improved corporate awareness across the organization. User involvement in the development of this application increased the perceived importance, for the designers, of application usability, quality and aesthetics. However, other initiatives within this organisation produced clashes with informal working practices and communities of practice. Within the second hospital, poor communication from IT about security mechanisms resulted in their misuse by some employees, who viewed them as a socially controlling force. Authentication mechanisms were used to socially exclude users who were formally authorised to access systems but whose access was unacceptable within some local communities of practice. The importance of users' security awareness and control are reviewed within the context of communities of practice.

Key words: Security, Privacy, Communities of Practice,

1. INTRODUCTION

Security and privacy have historically been strongly entwined with policy making, and hence top-down decision making. The argument that the 'user is not the enemy' (Adams and Sasse, 1999) is a response to the widespread authoritarian approach to security that views users as the enemy within, producing clashes between security concerns and users' goals and work practices. Taking a contrasting view, the field of HCI has foundations in user-directed issues, and therefore advocating user-centred security and privacy design (Ackerman and Cranor, 1999; Riegelsberger, Sasse and McCarthy, 2003; Whitten and Tygar, 1999) based on an understanding of users' perceptions of privacy and security (Bellotti and Sellen, 1993; Adams, 1999a, 1999b, 2000; Adams and Sasse, 2001; Lederer, Dey and Mankoff, 2002; Jackson, Eye, Barbatsis, Biocca, Zhao and Fitzgerald, 2003). Recent privacy papers have started to link social context, technical and policy issues (Ackerman, 2004; Palen and Dourish, 2003). However, the relationship between privacy and communities of practice is still unclear. This relationship is the focus of this paper.

Communities of practice can act as a link between the end-user and organisation through the day to day working practices of work-based communities (Wenger, 1999). Within the clinical domain, communities of practice exert a strong influence on both formal and informal work practices (Adams, Blandford and Lunt, in press). The clinical domain also presents interesting security issues (e.g. highly sensitive data) because of rapid technological developments that are designed to support effective clinical decision making (e.g. telemedicine, electronic healthcare records). However, the hospital setting, in particular, is very hierarchical in nature, and many users have negative perceptions of technology, poor IT skills, little flexible time, and poor access to technology and support (Adams and Blandford, 2004). The findings of this paper reveal the importance, for security within the clinical domain, of communities of practices as a link between end-user and organisational perspectives.

The focus of this research was to identify what end-users identified as crucial issues that impacted upon their information and technology usage within the social and organizational context of the clinical domain. This research opportunistically identified users' security and privacy perceptions free from the bias of the research question focus. It also highlighted the relative importance of these issues for users in the context of their other non-security related concerns. Distinct differences were found between participants' perceptions of security and its importance between the two organizations studied, where contrasting corporate approaches had been taken towards these issues.

2. BACKGROUND

The culture of the security domain determines the type of security problems identified and the approach to potential solutions. Historically, the security discipline focused on malicious intruders and technological solutions rather than users' perceptions, usability issues or the organisational role. This focus produced technical solutions that were both unusable and inappropriate. Recent approaches have understood this and sought to unpack users' perceptions of privacy and to provide guidance for system design. However, the gap between organisational approaches to security and research into user directed security is still evident. Reviewing the users' role within the organisation, and thus communities of practice, may give some insight into ways to bridge the gap. To set the scene, we start by defining some key terms: security, privacy, data subjects and data users.

For the purposes of this paper, security and privacy concerns centre around who can access personal information about an individual. If that access is for unauthorised or inappropriate viewing, the individual's privacy may be compromised; if unauthorised changes can be made to the data then that comprises a security violation. Two other security issues are touched on briefly: safety from attack (personal security) and unauthorised access to non-personal information without payment. Since the focus of this work is on unauthorised access to personal information, which compromises both privacy and security of data, the terms 'privacy' and 'security' are sometimes used interchangeably. One over-riding privacy and security (i.e. authentication) issue is clearly defining information ownership and usage.

Privacy literature often defines the individual whose privacy requires protecting as the *data-subject* and the organisation (including individual and communities within that organisation) using the data as the *data user.* Raab and Bennet (1998) have argued that this is a rather one-dimensional view of the *data subject* failing to acknowledge that data subjects' perceptions of privacy invasion risks may differ (personal exposures to risk, perceptions or fears of risk) across social groups and sectors (e.g. some socio-economic backgrounds being more vulnerable). However, we would suggest that although *data-subjects'* perceptions may vary across social groupings and cultures there may also be some unifying perceptions which would be useful to identify for privacy protection purposes. Many of the privacy debates that continue at this level centre on the *data- subjects'* awareness of information practices.

2.1 Security and Privacy mechanisms

Ackerman (2004) breaks privacy mechanisms down into 4 main categories: encryption mechanisms, anonymizing mechanisms, infrastructures, and P3P (the platform for privacy preferences). Encryption, it is argued, can provide security, but not necessarily privacy, while anonymity can encourage anti-social activities. Hong (2004) has proposed an advanced application of infrastructure (or software architecture) to support privacy aware software systems. However, to date, such systems only support simple privacy preferences. Ackerman (2004) argues for protocols that allow users and organizations to specify their privacy-related preference settings. This approach can provide a vocabulary for detailing the consequences of disclosing personal information and when this may be collected; P3P is probably the most widely used example.

Encryption and anonymity mechanisms are two different approaches to protecting data and identity, and attention has been paid to the usability of both. For example, PGP is a popular document transfer encryption tool that claims its interface allows novice computer users to utilise complex mathematical cryptography. However, Whitten and Tygar (1998) identified several usability issues arising from the metaphors used which encouraged users to develop inappropriate assumptions about the interface. Anonymizing mechanisms pose various challenges to application personalisation; Cranor (2003) presents three alternative approaches to enabling people to have personalised interactions while remaining anonymous, namely the use of pseudonyms, client-side logging of information and the development of task-based profiles. However, further work is needed to develop interfaces that support more usable and flexible control for users.

The platform for privacy preferences (P3P) provides a technical mechanism for ensuring that data is released only under an acceptable privacy practice agreement between the end-user (or data subject) and the web site (Cranor and Reagle, 1998). To reduce user effort, the proposal can be automatically parsed and compared with the users' preferences by a semi-autonomous agent (Ackerman and Cranor, 1999). However, time and effort are still required of the user to initially define the preferences.

Many of these mechanisms create overheads for users or require unworkable user behavior. It is therefore hardly surprising that many users try to circumvent such mechanisms. Part of the problem may be that many of the mechanisms are grounded in the notion of personal information and personal identity. While this serves as a starting point for privacy research it does not cover the complexity of privacy issues. The problem with many definitions of *Personal Information* is that they concentrate on the data itself rather than how it is perceived (Davies, 1997). As Agre (1997) points out, information is not a commodity, but is strongly embedded in the way we live our lives. It must be remembered that a notion of the individual and his or her relationship with society is pivotal to the privacy concept (Wacks, 1989). For us to be private, there must be a public environment. Privacy, and thus being private, can only be reviewed within that public context (Goffman,1969; Agre, 1997).

2.2 User Perceptions

To date, security experts have concentrated on protecting the individual against a malicious invasion of privacy. This perspective suggests the roots of a potentially adversarial relationship between security and user communities. In practice, many invasions of privacy encountered by users (as data subjects) are unintentional, poor interface design being a key factor in creating the possibility of unintentional invasion of privacy (Adams, 2000; Adams and Sasse, 2001).

Ultimately privacy, like trust, is reliant on our perception of it. It is not necessarily important how private or safe we are (although this is a vital component) but whether *we perceive ourselves* to be safe and private. If mechanisms and policies are based on inaccurate perceptions of users' privacy, they will not address users' current and future fears, and may further complicate matters.

The importance of an individual's ability to control data about themselves is central to many privacy approaches. Bellotti (1996) refers to this as the *operational* privacy definition which focuses on end-users' capabilities to retain privacy via access control and feedback. Bellotti and Sellen (1993) identify 4 factors that affect control and feedback mechanism design:

1. Capture – what kind of data is being picked up; voice, work activity and products such as key presses
2. Accessibility – who has access to the data
3. Purpose – to what use the data is put
4. Construction – what happens to the data (e.g. stored, manipulated out of context).

With careful privacy related design, users should have increased control of personal data, and thus privacy (Bellotti and Sellen, 1993). This, in effect, produces self-regulation of potential privacy invasions. One serious shortcoming of the control and feedback approach to privacy is that it relies on the assumption that users have the ability to identify what, by itself or mixed with other data, could produce a potential invasion of privacy. Bellotti and Sellen (1993) suggest that it is dangerous to rely on social and organisational controls of *Personal Information* or trade-offs for perceived benefits. However, it should also be noted that these are important factors when assessing privacy issues. Not only can these factors directly affect privacy; they can also affect users' perceptions of privacy invasions.

The Adams model of users' perceptions within multimedia communications (Adams, 1999a, 1999b) presents the *User* as the person who has data transmitted about themselves (i.e. the data subject). The user may not be actively using the system, and may be unaware that their data is being transmitted (Bellotti and Sellen, 1993; Adams, 2000). Primary to this model is the concept of *Information Sensitivity* (i.e. users' perceptions of the data being transmitted). This is reliant on the user's judgements of the sensitivity levels of the information being broadcast which are not binary (private / not private) but multi-dimensional. Also key to this model is the user's perception of who receives and / or manipulates their data (*Information Receiver*) and what they perceive it is used for (*Information Usage)*, both currently and at a later date. Each of the privacy factors interacts with the others and with contextual issues to form the user's overall perception of privacy. Lederer *et al* (2002) highlight the limitation of this model, in that the concept of context is vague and requires expansion to enable effective application of the model. A further model is developed that combines the Adams model and Lessig's economic model to identify perceptual issues that can lead towards a technical mechanism for providing control and feedback (Lederer *et al*, 2002).

Palen and Dourish (2003) base their privacy framework on identifying the boundary between privacy and publicity, either of which may be beneficial depending on the context. Four issues are identified as being important for designers:

- social and organisational context,
- temporal factors from actions in that context,
- possible threats from information usage, and
- trade-offs made by the user.

All of these models further the knowledge base of users' perceptions of privacy. However, they review privacy issues at the level of the individual within a social context. Resulting recommendations, policies and applications thus rely on the user being able and willing to interpret their privacy preferences and to evaluate risks.

2.3 Social and organisational approaches to security and privacy

Privacy can be driven by many different forces such as society, legislation, organisational policies, structures and culture. An overview of these forces can help us understand the different contexts surrounding privacy (Kling, 1996; Adams 1999a, b; Adams and Sasse, 2001). Many of the privacy debates at this level centre on the user's awareness of information practices.

It has been argued that making everything within society public would destroy problems associated with secrecy. Brin (1998) maintains that privacy can only be secured by increasing the *freedom of information* for everyone. However, there are three important flaws to this approach. Firstly, for this approach to work, there must be a utopian world where all information is free for access by everyone. As Clarke (1999) argues, there has always been a disproportionate distribution of power, with some people always having more power to avoid privacy laws or the call for *freedom of information.* Secondly, some information is inherently private in order for us to have our freedom of expression exempt from social scrutiny (Schoeman, 1992). Finally, the *transparent society* argument relies on secrecy being the main cause of privacy invasions. However, this assumes a limited concept of information, denying its ever changing nature. Different people can interpret the same data differently (e.g. jargon or 'within group' language could be misinterpreted by outsiders). Making information public could change its nature, and thus the *freedom of information* would be the very cause of privacy invasions [Palen and Dourish, 2003].

Bennett (1992) argues that the purpose of privacy legislation and policies is to increase trust in technologies and organisations through procedures to *take the lid off* personal data-processing media. However, although privacy advocates seek to increase users' (*data subjects'*) trust, they also argue that individuals are less able to evaluate the big picture of privacy protection and potential invasion of their data (Reidenberg, 1993; Bennet, 1997). This is completely at odds with the approach of privacy mechanism designers.

A major doctrine in security is the *need-to-know* principle (Adams and Sasse, 1999; Parker, 1992). The assumption is that the more that is known about security (authentication mechanisms, organisationally defined information sensitivity levels, privacy procedures), the easier it is to attack; restricting access to this knowledge therefore increases security. End-users (both *data subjects* and individual *data users*) are often told as little as possible because security departments see them as "inherently unsafe". While this strategy may be necessary in some areas of security work (i.e. limiting publications of browser and operating system vulnerabilities until a patch has been created) it may not always be the best approach when dealing with the user community. It has been argued that this approach decreases users' security awareness and security departments' knowledge about users, thus producing poorer security systems. Ultimately, the culture within which technology is situated can determine aspects of its use (Dourish, 1993; Harrison and Dourish, 1996). Certain technologies may apply well in an environment of trust but fail in an atmosphere of distrust. For example, the media space at Xerox PARC operated on a 'sign-up' basis, whereby those that opted in to the application were considered to accept the social practices and norms which governed acceptable use of the space (Dourish, 1993). However, this assumes privacy invasions only occur through *intentional* acts of inappropriate behaviour. Is trust the central issue, or is it a case of awareness and communication?

There has been a recent increase in articles that seek to support designers in privacy aware design (Lederer, Hong, Dey and Landay, 2004; Palen and Dourish, 2003) and to bridge the gap between organisational and user perspectives (Lederer *et al*, 2002). However, often these approaches fall into the trap of only designing for the individual and not for the group. Community privacy requirements and support have not been explored in great detail, and may introduce a link between organisational and individual approaches to privacy. Harper (1992) proposed that a person's attitudes and perceptions are intimately related to the role they have within the organisation. How technology is used is determined by what a user does within an organisation, their formal position and the state of their relations with others. Applications which merely preserve and reflect the pre-existing status quo of data distribution and usage will be more acceptable than those that change individuals' relations with others. Ultimately, this links into the relationship between individuals' privacy concerns and those of communities of practice within the organisation. However, there are tensions between maintaining systems that fit with current work practices and the growing legal and social requirements for changes to meet security needs. The issue that is central to this paper is how those changes are implemented and negotiated between security professionals, individuals and communities of practice.

Traditionally most security initiatives within organisations relate directly to the individual through policies, email and memo notifications. We argue that open communication about security requirements within communities with security professionals can help the community understand security risks and drives for changes while increasing motivation to adhere to changes in work practices. Conversely, through consultations, security professionals can identify current informal work-practices and associated security and privacy risks and adapt systems to increase security while reducing changes to work practices.

2.4 Communities of Practice and the Clinical Domain

Raab and Bennet (1998) refer to the concept of *personal grouping data* as placing an individual (data subject) within a group. This can increase the sensitivity of the data (for the data subject), as judgements about an individual may be based on information about the group (e.g. a persons known as 'White American' can be sensitive data but when linked to that of a reading group's topics of 'apartheid' and 'the Nazis' increases the sensitivity of the data than if they were 'Black American'). Some social psychologists make the distinction between the personal and the social identity (Auoustinos and Walker, 1995], where the former relates to characteristics that are strictly individual and the latter to an individual's position within a social group. It is important to understand how communities impact upon the sensitivity of the data subject's information and the security of how the data user utilises the information within organisations. With the former, communities of practice can help us understand how to devise mechanisms to support both individual and community privacy needs. With the latter this approach can help bridge the gap between different security and privacy goals of the individual and the organisational data user. The studies presented in this paper deal with both these issues, but primarily the latter.

Technological developments are increasingly focusing on the importance of directing design towards the work practices and communities they support (Covi and Kling, 1997). Supporting communities of practice can assist the development of effective ways to share knowledge across organizational boundaries, thus promoting collaboration and coordination while also increasing productivity and organizational performance (Millen, Fontaine and Muller, 2002). The concept of 'communities of practice' emerged from a learning theory developed by Lave and Wenger (1991) called 'legitimate peripheral participation'. According to this theory, learning within any domain is more than a formal acquisition of knowledge or information: it has a social element which is often ignored. Learning, it is argued, should take place through a process of participation in '*communities of practice'*. The theory details how new members are brought into knowledge communities, and how these communities both transform and reproduce themselves. This participation is at first peripheral, but gradually increases in both engagement and complexity. Wenger (1999) extends this to a framework in which the two basic streams are *Practice* (from collective social norms of practice to accounts of meanings) and *Identity* (from impacts of organizational power and social structures to those of personal subjectivity).

Communities of practice can act as a link between the individual and organisation through the day to day working practices of work-based communities (Wenger, 1999). Within the clinical setting (the focus of this paper), Reddy and Dourish (2002) identified the importance of communities and colleagues in providing support for information seeking behaviours; they found that colleagues typically provide the contextual information and interpretation that is absent from published information. Similarly, Schneider and Wagner (1993) highlight the importance of local knowledge, informal collaboration and technology to support the sharing of information within the clinical setting. This view is echoed by Cicourel (1990), who notes that team members on medical ward rounds provide contextualizing information to each other. It is useful to understand therefore that as data users clinicians work collaboratively with the data. However, there is little research which reviews privacy data and security mechanisms with regards to communities of practice. The exception is the importance that informal work practices (a key concept of communities of practice) have on security mechanisms, as highlighted by Adams and Sasse (1999).

Both formal and informal work practices help to develop rich and varied social interactions in the modern workplace (Millen *et al*, 2002). Adams and Sasse (1999) found that systems which do not take into account informal work practices, and are perceived to restrict those practices, will be circumvented. An organization's culture has a direct impact on the informal practices that can develop into social and organizational norms (Schein, 1990). The distinction between formal and informal work practices is generally clear, but can be even more important for health care systems than most others. When hospital information systems were first introduced, it was found that the greatest difficulties in their deployment lay not with technical issues but with the end-users, on whom new demands were being placed (Harrison, 1991). Recent health informatics research also reveals that social and organizational factors can determine the success or failure of healthcare IT developments (Harrison, 1991; Heathfield, 1999). Heathfield (1999) suggests that this is due to the complex, autonomous nature of the medical discipline and the specialized approaches to system development (which are typically led by either a clinician or a software engineer). The diverse organizational culture of hospital structures, made up of many different professions with their own specific social identifiers, can often produce conflicts between those professions (Morgan, 1991). Symon, Long and Ellis (1996) found conflicts within a clinical setting relating to social status and information practices. For example, higher status professionals were found to be more concerned with keeping their social status as an expert within the organization than adhering to formal organizational norms. It is important to understand these social pressures when devising security mechanisms. Very often security mechanisms and privacy policies are devised according to formal work-practices that simply don't fit those within the organisation (Adams and Sasse, 1999; Adams and Sasse, 2001).

3. METHOD

The focus of this paper is on how security, privacy and communities of practice relate to findings from the clinical domain, and, in particular, from studies conducted in two large teaching hospitals. The organizational structure of both hospitals studied is complex, hierarchical and undergoing dramatic change. Funding restrictions mean facilities are limited and under-resourced. Technology provision varies greatly; however, the majority of clinicians do have access to a computer, even if that computer is shared. Most end-users have limited computer skills, although abilities vary quite dramatically. Many clinicians are resistant to change, particularly technological change; this resistance is due largely to a poor understanding of how applications can support, rather than hinder, current working patterns.

3.1 Study 1:

One study was conducted in a provincial teaching hospital. In this hospital, most of the computers were in offices and the library, and allowed access to the web. There were still some dumb terminals on the wards that provided access to specific administrative applications. Privacy and security was not only initiated by national directives but also by local issues, and implementation was driven by the privacy officer and security team. 20 in-depth interviews were used to gather data from clinicians (i.e. nurses, consultants etc.) management, library and IT staff (see table 1).

3.2 Study 2:

The second study was based in a London teaching hospital. In this hospital, computers have been placed on the wards, with web-accessible digital libraries. Privacy and security was directed by national directives. However, community specific issues were not identified and security and privacy issues were low on the local agenda. Focus groups and in-depth interviews were used to gather data from 73 hospital clinicians. Approximately 50% of the respondents were nurses while the other 50% were junior doctors, consultants, surgeons, Allied Health Professionals (AHPs; e.g. occupational therapists), managers, and library and IT department members (see table 1).

Table 1. about here.

3.3 Data Collection and Analysis:

As noted above, data collection was based on interviews and focus groups. Four issues guided the focus of questions within all the studies:

- Perceptions of the individual's role within the organization, and their information requirements.
- Perceptions of current information practices, social structures and organizational norms.
- The impact of current practices, structures and norms on information resource awareness, acceptance and use.
- Technology perceptions and how these affect other issues already identified

The researcher did not specifically ask about or introduce security issues. Any privacy or security issues highlighted were introduced by the respondents themselves as being important and relevant. Thus, the security and privacy issues highlighted here were perceived as being of paramount importance to the participants.

An in-depth analysis of respondents' perceptions was conducted using the Grounded Theory method. Grounded Theory (Strauss and Corbin, 1990) is a social-science approach to data collection and analysis that combines systematic levels of abstraction into a framework about a phenomenon which is verified and expanded throughout the study. Once the data is collected, it is analyzed in a standard Grounded Theory format (i.e. open, axial and selective coding and identification of process effects). Compared to other social science methodologies, Grounded Theory provides a more focused, structured approach to qualitative research. The methodology's flexibility can cope with complex data, and its continual cross-referencing allows for grounding of theory in the data, thus uncovering previously unknown issues – such as the privacy and security matters presented here.

Further quantification of the data is also provided by breaking the security and privacy issues down further into sub-issues. The percentage of general security and privacy issues identified within each study is presented as well as the percentage of each specific sub-issue (those issues identified within both studies are compared and those specific to each study are presented separately).

In the qualitative results discussed below, many points are illustrated with verbatim extracts from the interviews and focus groups. In these quotations, the speaker is identified by role, but not as an individual (so, for instance, multiple excerpts from a 'Pre-registration nurse' are not necessarily from the same individual).

4. RESULTS

The two different organisational approaches to security (i.e. primarily authentication and access rights) and privacy for clinicians resulted in different perceptions of security and privacy. Within both the organisations clinicians were primarily data users of sensitive patient data. However, with the growing importance of 'clinical governance'[1] the auditing and tracking of clinicians' daily activities and decision making procedures has vastly increased. The amount of personal information stored about clinicians' daily activities has increased the degree to which they are not only data users but also data subjects. Our findings highlight how the different approaches to security and privacy changed users' perceptions of privacy and security procedures in their role as users of patients' sensitive personal information. However, these different approaches also changed clinicians' perceptions about organisational usage of their personal information as data subjects.

In study one, awareness of privacy policies and procedures was high across all users (consultants, doctors, nurses and management). In general security and privacy procedures were viewed as a protective mechanism for communities, in particular patients. In study two, security awareness and privacy policies as data users was poor. Clinicians became more aware of personal access to information and personal privacy with regard to organisational auditing of their behaviours. In general security and privacy procedures were viewed as a defensive personal weapon (by those of a higher status e.g. consultants, doctors) to exclude individuals (those of a lower status e.g. nurses, patients).

Three important themes emerged from the data regarding security and privacy policies and the structure of communities of practice within the organisation:

- Circumvention of access procedures and privacy policies that are not owned: Established communities that did not 'own' a new security protocol were found to circumvent it or actively oppose its introduction.
- Security mechanisms creating social divisions: Security issues were sometimes distorted by communities within an organisation and used for their

[1] The governance and accountability of clinicians and clinical bodies for clinical decision making.

own ends (e.g. to reinforce existing hierarchies and distinctions between groups).

- Community ownership: IT engagement between security and those in clinical care supported empathy on both sides and constructive development of solutions for all.

We consider each of these themes in turn.

4.1 Circumvention of procedures that are not 'owned'

Within study 1, there was a report of a clash between one community of practice (in this case, clinicians as users of patient data) and another (the security team). Users within other domains might have circumvented procedures they felt were inappropriate, but the clinicians expressed their dissatisfaction directly and actively. One incident, described by the privacy officer, concerned a computer room that contained very sensitive data. The room was only accessed by clinicians but it was at the end of a corridor occasionally accessed by the public. The IT department decided that as this data was particularly sensitive there was a need for increased security for this room. The security for the door to the room was therefore increase to be one that automatically closed and locked. All the relevant clinicians were provided with keys and informed of the reason for this new procedure being put in place. Some clinicians, however, felt this change in practice was 'paranoid' and uncalled for and so kicked the door down to this room.

> *"…I had a problem with the clinician stamping their feet, kicking the door in, swearing at me"* **(Privacy Officer: St1).**

Although the vandal was not identified consultations between the IT department and clinicians resulted in the computer room and its security (i.e. locked door) being reinstated. Poor communication was identified as the main problem and new processes (e.g. committees, email debates) to communicate between the hospital and IT staff was a direct result of this episode.

It was realized by the security team that what appeared to them to be a simple security issue had produced very emotive responses from some clinicians. Further discussions ensued that allowed the clinicians, as data users, to have a forum within which to voice their concerns about required work practice changes. It was identified that the security team's identification of a potential problem and resulting solution was not 'owned' by the community to whom it mattered. Further communication with and participation of the clinicians in security issues were deemed necessary to resolve potential confrontations in the future.

4.2 Security mechanisms creating social divisions

Within study 2, matters regarding security were dealt with less confrontationally, but nevertheless proved to be divisive, albeit in more subtle ways. Many of the security issues were exacerbated by the physical location of the IT department (across the road from the hospital), which increased communication problems. System development was either directed by national policies or by high ranking clinicians within the hospital championing their own agendas. As security had not been taken up and championed by anyone as a specific point of concern, it was considered a lower priority than other system development issues.

Within this hospital, vague government privacy policies and procedures were adhered to in principle, but in practice they were often breached in their execution. The location of computers meant that sensitive data (both patient data and clinicians' personal data) could be glanced at by members of the public over someone's shoulder, while departmental whiteboards and paperwork (sometimes accessible at the end of beds) contained patients' personally identifiable data. Clinicians (both doctors and nurses) reported that they viewed security as a barrier rather than a protective mechanism. Problems with communication meant that these barriers were, intentionally or otherwise, socially divisive. Overall, the lack of communication about security matters resulted in local communities of practice adopting security-related issues for their own ends (e.g. to maintain current social structures). Various examples of this general phenomenon emerged through the data.

One example was poor feedback on ownership and support for different levels of security authentication on the staff intranet. This intranet provided resources that were internally useful. Politically, there was an established 'pecking order' of what information could appear on high-level pages within the intranet. It was discovered that one top-page link presented the name 'OVID' without any explanation of what it was. OVID is a digital library authentication mechanism used verifying access is restricted to hospital employees rather than the public in general. The link had been championed by a top-ranking clinician who liked the service, as did his colleagues. The link took the end-user through to an authentication page used to restrict access to hospital personnel regardless of whether they were accessing the site from the hospital or home. However, the authentication page provided no feedback on what the resource was for or how to get support for the authentication process (e.g. where to obtain passwords from, or explaining the difference between user ID and password). Screen real-estate restrictions on the top-page stopped IT services from providing more information for the link. Background information and support links could be provided on the authentication pages (which was the resulting compromise). However, potential users who did not know what OVID stood for were unlikely to access this link in the first place. It was suggested that contextualizing the link within the library service pages would support users' understanding of it (e.g. what the service is likely to be, who is likely to support it and provide passwords). The library, however, was considered of too low standing to be represented on the top page of the intranet. The usability of the OVID authentication (security) feature was compromised by the tension between the status of the sponsoring clinicians and that of the library within the organizational structure. This is an example of how necessary security mechanisms can be misused in order to maintain differences in power between individuals with differing. Increasing authentication usability may be easier in theory, out of context, than within organizational settings.

Other manifestations of the same broad phenomenon were apparent throughout the organisation. Poor communication from the IT department about security mechanisms provoked their misuse by some employees, who viewed them as a socially controlling force. Authentication mechanisms were used to exclude users who were, from an organisational standpoint, authorised to access systems but whose access was unacceptable within some communities of practice.

> *"... But they put a block down on that because they've said 'well if one student nurse gets to use it then all the student nurses will want to use it'."*
> **(pre-reg nurse: St2a)**

Nursing staff reported that the physical location of the computers within this hospital limited their accessibility. Senior staff members were reported to use security risks (e.g. theft, damage, unauthorized access) to justify changing the physical location of computers, which reinforced existing power relations and excluded nursing staff from accessing systems.

> *"I know that there is one computer on the ward which is supposed to be for everyone to use it but because it's in the doctor's office, they don't want people in there in a certain time because they could be putting something on tape, doing their notes. So it ain't for everyone is it."* **(post-reg nurse: St2a)**

Government health privacy policies are vague but refer to the protection of sensitive data by restricting access to this data (e.g. authentication procedures, location of computers containing sensitive data). Issues such as personal patient information on whiteboards, the location of computers that retain sensitive information, is however, an issue that hospitals are slow to deal with in practice although they often say these are being dealt with in theory. To increase effective healthcare the patient information entered on the computer should be accessible by both doctors and nurses. The data was secured, according to the law and hospital privacy policies, by password protection and as such the hospital deemed them secure on the wards. The same data was identified as often duplicated on paper based notes left in semi-public locations (e.g. nurses' bay on the ward) and in some hospital departments hanging at the end of the patient's bed. In some departments dumb terminals with patient data were on the wards while other terminals were locked in doctors' and nursing managers offices. The key difference was the Internet accessible capabilities of the technology which was noted by the nurses as the reason behind the restrictive actions of the senior clinicians.

The IT department were, in contrast, eager to increase computer accessibility, and had negotiated Internet access for all users within the organisation. A national directive had, at the same time, dictated that everyone from a janitor to a consultant should be given access to email accounts. However, when clinicians were interviewed, their understanding of when and how they could access the Internet was poor. Senior clinicians were noted as using this poor authentication awareness and social structures as a barrier to accessing general medical knowledge. For example, one nursing manager detailed a long procedure that she had to go through to be granted a password.

> *"I have access because I'm studying for a further PhD anyway and I think this job is where I actually need that information so I have access but it had to be granted by the director ... As things stand at the moment 4 pieces of paper had to be signed before I could actually get it."* **(Nursing Manager: St2b)**

Once she had a computer and Internet access, she was then not aware that this access was unlimited, and consequently restricted her usage to out of office hours.

One justification given by senior clinicians for restricting access for junior clinicians was their ability to interpret this information like the senior clinicians could. A few examples of this justification from different participants are:

> *"... there may be stuff in this country that is of a reasonable quality but it requires some skill to some extent to be able to discriminate. I*

> *don't have difficulty with this. I don't know how much the nurses or the junior doctors would be able to discriminate."* **(Consultant: St2b)**
>
> *"... you find that people will just go off and they will misunderstand the national guidelines because they come out in long documents which interpretation requires further study. So I think for junior doctors they can be misleading, harmful, damaging."* **(Consultant: St2b)**

The restriction of information (primarily general medical literature) made available to junior clinicians was a theme throughout this organisation, as was the use of security mechanisms as a socially divisive weapon. All the junior staff members (i.e. nurses, AHPs and doctors) considered computer technology to be an essential tool for completing their jobs effectively. Nursing staff (especially student nurses) and AHPs perceived it as an 'empowering tool', providing them with the information and knowledge that they required to complete their jobs effectively. However, many senior staff members expressed a desire to retain their expert status by continuing to control information dissemination procedures. Some senior staff argued that they would rather access digital resources on behalf of junior staff.

> *"... if they want something on this or that then I'm around to do it for them."* **(Nursing Manager: St2b)**

Junior staff argued, however, that as well as this wasting valuable time for senior staff, security protocols dictated that a third party (in this case, the more senior member of staff) should not have access to personal or private information (i.e. general information searches on patients specific conditions and personal circumstances e.g. juvenile sexually transmitted diseases) that *they* did not need to perform their duties. Security procedures (in particular authentication mechanisms) were therefore being used by both senior and junior clinicians to justify restricting computer and information accessibility. Further details on technology and social empowerment and exclusion can be found in other publications (Adams, Blandford & Lunt In Press)

4.3 Community development of a screen saver application

Although security and privacy management can, as illustrated above, create tensions and reinforce social divisions, it can also be used constructively to create greater community cohesion. Within study 1, there was an example of effective community-based system development to address the issue of privacy protection (primarily for users of patient information).

Within hospitals, sensitive data is continually being used on PCs in public and semi-public spaces (e.g. wards and offices where patients are diagnosed), so there are privacy policies in place to ensure protection of sensitive data. Computers left unattended should have password-protected screen savers restricting access to sensitive data. However, in practice many data users in both hospitals were not using password protection, and this was growing harder to police. Those that did use personal screen saver passwords inhibited effective hot-desking practices:

> *"if a secretary was off sick or went on Annual Leave then when somebody came in if they weren't aware that the screen saver was initiated on the machine it kicked in and all their work behind it was lost because the only thing to do with it was to switch the machine off."* **(Screen Saver development team: St1)**

The hospital's approach to these problems was to employ a privacy / data protection officer within the IT department. An IT security team (led by the privacy officer) then devised a corporate screen saver that appeared on every inactive PC throughout the hospital. The system would cycle through IT security advice screens (see fig 1) that gave information on securing personal data, incident reporting etc. Further details of this system design and implementation are detailed in a specific in-depth publication (Adams & Blandford, In Press)

Figure 1 about here.

However, as end-users became desensitised to security issues (e.g. 'oh that's just security stuff; there's no point in reading them') they decided to display screens from different community user groups within the organisation. Important organisational news was highlighted (e.g. training sessions, availability of new resources, winners in organisational sweepstakes). It was decided very quickly that the content of these screen savers should be restricted to information that was of organisation wide importance. Subsequently, security issues remained a primary topic, with additional screens from user groups across the hospital. In total 112 user groups across the hospital (many of whom have contributed screens) have been in consultation with the screen saver project developers. There were so many user requests for screens that the developers decided to specify that no image could be displayed for longer than a month, and to refuse requests from external bodies. As user interest increased, so did the importance of usability issues for the development team. Developers placed guidelines on the Intranet for usable and successful screen saver construction. Complaints from users who missed screens in the cycling process led to screens being made accessible via the Intranet. This, in turn, led to the development of screen savers with contact details for where further information could be obtained (e.g. via telephone, email, on the Intranet).

Overall, the screen saver application was identified as reducing problems of communication while increasing users' security and organizational awareness. It was noted that this was particularly due to the passive quality of the application:

> *"The thing that is good about this is even if people don't use the PCs they'll walk past the PCs and see them."* **(IT manager: St1)**

Information for the screen savers were mediated by the security personnel of the IT department. Meetings were established with different user groups to discuss screen saver information content. In the process of these meetings security and privacy issues were brought up (by both IT and user groups), discussed and further changes to policies introduced. Some of these issues related to specific user groups (e.g. policies around notification and collection of doctor referrals received by general access fax machines) and some were hospital wide issues (e.g use of anonymised labels for printed patient information transferred to other departments). Notifications of final changes made were introduced through new screen savers.

As well as the 'idle' screen saver, an urgent notification system was also deemed necessary. Various incidents, such as attacks on clinicians, had led to the requirement of a system that could interrupt end-users' activities to alert them to immediate security risks (e.g. intruder alerts, attacker alerts). As this was not simple to achieve through the screen saver application, it was decided that a separate program would be developed to support this need. The resulting 'traffic lights' system made it possible for a message to be sent out which was immediately displayed in front of the user's current work. The message remained until the user actively cancelled it, thus acknowledging that they had received it.

> *"you can't disregard it, you can't get rid of it until you've read it because you actually have to click it off which I suppose is really good in the way that when, with the consultant's attack, we needed to get a message out urgently, with his description, we could do that... So it's a way of getting something out there if you want them to know within minutes."* **(Screen-Saver development team: St1)**

The development team again consulted with user groups and noted concerns that the level of disturbance this system provided was very high. It was therefore decided to restrict the use of this application to very important messages. The system had two primary purposes:

1. Urgent messages e.g. details of a staff attack.
2. Reports on hospital bed status – one a day. (see fig. 2)

Figure 2 about here.

The 'traffic lights' system was cited by many as a controversial yet positive application throughout the hospital. It was perceived to increase awareness across the hospital trust by keeping people in contact with the organisational status:

> *"People on the management corridor were unaware of anything untoward going on and it can be like a war zone in AandE with like 20 patients waiting. There was no feedback, no feedback loop."* **(IT / Admin: St1)**

The screen saver and 'traffic lights' project created an interaction between the IT department and communities of practice that had never occurred before. This interaction increased not only user involvement and ownership of the systems, but also users' security awareness. Respondents described, without prompting, specific security and privacy procedures they followed with regard to data usage or that they felt were not being upheld by third parties (e.g. anonymized patient labels).

A larger number of users in study one spontaneously highlighted security and privacy procedures as a protective mechanism for different communities (patients and their information, clinicians and their personal safety) than did within study two. This increased communication and also improved the IT department's awareness of user issues. The privacy officer, in particular, noted the need to understand user motivation when dealing with general security education.

> *"but we keep going out there and saying we want this and that and we want to change this and we want to do that and you know, I'm starting to think they're going to think yeah but there's nothing in it for us"* **(Privacy Officer: St1)**.

Future computer security initiatives were being devised that tapped into user and community motivations while raising security awareness. A security award scheme was devised that would introduce IT security and privacy through online security information courses. Awards would be given to communities such as wards, and advertised throughout the organisation to increase community pride and motivation.

> *"an information governance award scheme so it's giving departments awards... and basically there's three awards, there's a bronze, gold and silver award ...if they think 'Oh, ward seven's got a bronze, I want a bronze'"* **(Privacy Officer: St1).**

4.4 Summary of Studies

In study one, clinicians were primarily data users (of patient information), and their role as data subjects (e.g. leaving traces through personal emails and personalised procedures) was relatively minor. Security focused on computer authentication and physical access, with organisational and community based privacy procedures and protective mechanisms (e.g. the screen saver application). Clinicians rejected new access restrictions, introduced without negotiation with relevant communities by the security department, for protection of patient information (e.g. locking the door to sensitive data). This was described by clinicians as another way to restrict their activities. Yet a corporate screen saver to protect patient information and clinicians' personal information, implemented through negotiation with different communities (i.e. doctors, nurses, oncology, radiology), was perceived as a protective mechanism. By working with the user community the security staff was able to build a solution that met their security goal of getting users to use the locked screen saver by having the solution also provide them valuable additional functionality in the form of increased communication and education. The development of this system raised awareness of security issues across the hospital. The authors' advice on the importance of communication with communities in the successful implementation of security and privacy procedures was noted by the IT department for future developments.

Within study two, clinicians were aware of their roles as both data users and subjects, although security (i.e. authentication and physical security) was of primary importance. Privacy policies for patient information were regarded as less important, and were often disregarded. Authentication systems (e.g. for Intranet and Internet usage) relied on a mixture of IP, local passwords and passwords for remote systems without clearly detailing the differences, or why and who was responsible for support. Clinicians were more aware of personal access to information and personal privacy with regard to organisational auditing of their behaviours. In general, security and privacy procedures were viewed as a defensive personal weapon (by those of a higher status, such as consultants and doctors) to exclude individuals (those of a lower status such as nurses and patients). From discussions with the authors, the security department has recognised problems associated with user awareness and involvement in security and privacy procedures. In particular, the hospital is considering implementing their own screen saver project to both increase privacy and improve communication with clinicians about security issues.

4.5 Comparative analysis of the studies

From the provincial hospital (study 1), 85% of clinicians highlighted a range of security and privacy issues, whereas in the Inner City hospital (Study 2) only 48% of clinicians identified such issues. Of this number, a far lower percentage of these issues were highlighted by the nursing than the senior clinicians and other professions (see table 2). However, it was the different types of issues that each hospital highlighted that indicated the different approaches to security within these two hospitals.

Table 2. about here.

When breaking the security and privacy issues down into sub-issues, there were three issues highlighted by both organizations: data security and protection in general; physical security; and the validation of information quality. There were substantially more people who highlighted these issues in study 1 than in study 2 (see fig. 3).

Figure 3 about here.

As well as the few common issues, each study also highlighted different issues. Study 1 highlighted a high percentage of issues related to perceptions of security as a protective device while study 2 highlighted more perceptions of security as a barrier and restrictive mechanism. These issues for which there was no overlap between the two studies are shown in table 3.

Table 3. about here.

5. DISCUSSION

Within the clinical domain, social structures and informal work-practices have been widely recognised as being central to effective operation. Reddy and Dourish (2002) identify one of the limitations of information technology as being the way it takes tasks out of context. Similarly, security mechanisms often ignore important contextual factors. Adams and Sasse (1999) highlight the difficulties created by people having individual passwords in a group working context (this issue also emerged in this study, as discussed above). This study has highlighted the need to understand users' work practices and the relevance of these within the context of communities of practice. Another important factor within this domain is the traditional distrust that technology often evokes (Adams *et al*, in press). As noted by Levy, Bradley, Swanston and Wilson (2001), technology within the health profession is slowly eroding senior clinicians' sense of power. 'Smart' decision support tools and tele-health facilities are seen as re-directing the information power to lesser-trained providers or to the patients themselves. At the same time, the nursing profession argues that technology is being used to strengthen existing hierarchical organisational cultures and status norms (Sandellowski, 1999). With this background and the fact that security is traditionally negatively viewed by end-users, it is especially interesting to understand why the screensaver described above was a success story.

Within the provincial hospital (study 1), the organisational approach to technology and security was to treat security as a high priority, so much so that a privacy officer was employed by the IT department. Although this is a very unusual approach within the UK health domain, it is common in many other domains. What makes this project stand out is that, despite security initiatives being both policy and technology driven, the project team also sought to support user needs (primarily as data users but also as data subjects). This is quite a common approach with regard to users' privacy mechanisms, but is very unusual at an organisational level. The P3P approach (Cranor, 1998, 2003; Ackerman, Darrell and Weitzner, 2001; Ackerman, 2004) does seek to increase communication, negotiation and agreement between the organisation (as data users) and user (as data subject) levels. However, this is primarily Internet based, and is meant for online transactions. The 'screen-saver' application developed by the provincial hospital was initially devised to protect organisational and personal security and privacy. Through the security implementers re-negotiating with different communities to establish agreed norms new policies and procedures, this application became a new communication medium, improving corporate awareness across the organisation. This has helped in establishing norms for privacy in usage of patient data, and initiated a debate on privacy with respect to the growing quantity of sensitive data on clinicians' activities (e.g. through audits and tracking of clinicians). The screen saver awareness application has now become a key tool for organizational communication within the hospital. It was noted that many working groups, when discussing dissemination or advertising procedures, would specifically state that 'I can feel a screen saver coming on' or 'we need to get a screen saver for that'. The quality of experience provided for users by a sense of belonging to the greater corporate whole, with a joint perspective on organizational goals, should not be underestimated. This ownership and sense of community was transferred to the different screens that appeared on the system. As the privacy officer had a key role in the system implementation and its upkeep, there was a large number of security awareness screens. This raised the profile of security, resulting in a larger number of the users interviewed within this hospital identifying positive security and privacy issues (i.e. accurate accounts of how to secure data and ensure privacy) when discussing information procedures than within the London hospital (study 2). End-user involvement in the development of this application also increased the importance, for the designers, of application usability, quality and aesthetics.

It has been noted that there is a need to move away from a top-down approach to security as it can provoke circumventing behaviours from users (Adams and Sasse, 1999). Instead, it is suggested that security should develop links with communities of users at departmental level to develop appropriate procedures that users are motivated to complete. The traditional authoritarian approach to disseminating organisational security and privacy policies is either via paper-based distribution or hidden in online security pages. These are often poorly attended to, and consequently awareness is disappointing. Within Study 1, an imaginative approach to raising security awareness was also taken at departmental levels via a community based online security training and award scheme. The notions of community pride and inter-community rivalry were identified as sources of motivation to acquire security knowledge and awareness.

It should be noted, however, that there were other less successful security initiatives within this organisation (e.g. locks on doors to sensitive data computer rooms, as described above) that produced clashes with communities and their informal working practices. An account of this reaction could be found in the 'control and feedback' privacy approach (Bellotti and Sellen, 1993). The previous security and privacy approaches this organisation took increased security awareness through feedback to communities. The communities became involved in the system development process, thus increasing their sense of ownership. However, the level of control that community groups had over security policy and procedure was very limited. This was evident with the door locking policy whereby again decisions were made by a central security department and the communities then informed. This brings back the concept of communication between security departments and users being restricted to a "ticking off" of users caught circumventing the rules. This approach antagonized many highly qualified clinicians trying to deal with safety critical situations in restricted time-frames. As previously argued, users have to be treated as partners in the endeavor to secure an organization's systems and its privacy policies, not as the enemy within (Adams and Sasse, 1999).

Within the London hospital (study 2), technology and security were considered a lower priority. Many security initiatives, specifically with regard to privacy policies, were directed by national policies within the domain. Although the IT department were eager to involve users in system developments, poor communication and inappropriate security mechanisms were perceived by clinicians (as data users) as a barrier to usability, overall security and privacy practices. Poor communication from the IT department about security mechanisms also provoked their misuse by some employees, who viewed them as a socially controlling force. In particular, senior clinicians used security risks as a reason to exclude junior clinicians' access – either by the physical location of the computers or by complex procedures to obtain passwords for online access. Junior clinicians retaliated with arguments of third party security with regard to senior information gatekeepers. The use of security procedures and mechanisms as a theoretical weapon between different communities can be negatively divisive. The result is typically that security procedures and policies are perceived by both groups as superficially important but not of any real relevance.

It is interesting to compare these two studies, as both hospitals were dealing with complex security and privacy requirements within a domain that does not co-operate well with technology or really understand the risks involved. Both of the organisations had IT departments that took security and privacy issues seriously. However, the outcomes within the hospital communities were very different. One cause of the difference was undoubtedly the appointment of a privacy officer who initiated local and department-specific privacy and security policies. However, it was the community approach of this officer that had the strongest impact on the outcome.

The importance of the interrelationship between security and organisational communities is an interesting field of research that requires further study. Within the traditional computer privacy paradigm, personal information relates to both information about an individual (name, etc.) and their social groupings (ethnic background, political / religious convictions, area in which we live, etc; Raab and Bennet, 1998). This highlights the importance of the individual's place within society. In the context of this paper there are communities of practice within the health domain (data users: doctors surgery, hospital teams, ward teams) that utilize individuals' personal information. The concepts of personal information and personally identifiable information are core to devising mechanisms and policies to protect this data. However, as previously mentioned people and their privacy cannot be understood in isolation but within communities. We are individuals who are integral parts of a community and these communities have practices that are both work and socially related (e.g. jobs, bringing up families). Privacy, in particular, is often not regarded as a concept associated with the community itself. However, it could be argued that the community **itself** has its own identity, which relates to the individual (Auoustinos and Walker, 1995). The notion of privacy could also be related to broader concepts of patient communities, with their own higher level privacy requirements (patient family privacy, work colleague privacy). Each group has valuable health information (data subject *groups*) that can be used to support diagnosis and treatment (e.g. communicable diseases in particular contexts). It could therefore be argued that each group or community has its own privacy requirements at a different level to that of the individuals' privacy.

According to Wacks' (1989) definition of personal information, if the information relates to the individual it could be personal information; however, the information relates indirectly via a community. For example, an individual might feel implicated by association if there was a negative report about some group with which they are associated. This would mean that even if an individual is anonymous, if the community is identified then the individual is indirectly identified. Highly sensitive data, therefore, may not only be personally identifiable data but also community data (e.g. a house identifies a family group; a street a geographically bound group; a school a social group). Social grouping perceptions, and in particular community relevant information, should be considered when reviewing privacy issues.

Within Britain, a recent advertising campaign highlighted this problem when its advertisements detailed a specific street (a social grouping) as containing individuals (not identified) who were breaking the law. People within the street who were not breaking the law reacted very negatively to this portrayal to the world of negative details about their street. Individuals could similarly find it invasive if sensitive information is made public about anonymous individuals from their specific school, church or social group. This brings to the fore the notion of a social grouping privacy. It could be argued that, as we become larger, more multicultural societies, the smaller social groupings we join which retain our beliefs, feelings and biases become more important. Technology, and in particular the Internet, erodes distance as a social grouping barrier and again raises the importance of the communities we join.

6. CONCLUSION

By considering the relationship between the implementation of security and privacy practices and communities of practice, the work reported here has highlighted the importance of end-user awareness of these practices and their ability to control them at a community level. Many of the social and organisational approaches to security and privacy deal with the important issue of users' awareness but not of control (Brin, 1998; Bennett, 1997). Even the security domain's 'need to know' approach has a consequence of reducing users' awareness as well as control (Adams and Sasse, 1999). Many privacy mechanisms deal with users' awareness through feedback, but also incorporate personal control of information and procedures. However, there is little understanding of the community role within these approaches.

Study one has highlighted the fact that, to effectively implement systems to protect organizational and personal security, there is a need to understand the social structure, norms and work practices within that organization. Study two in contrast highlighted that organisational security and privacy policies developed and implemented without community involvement will increase perceptions of security and privacy mechanisms as a weapon to be hijacked for divisive purposes. Security issues such as trust and privacy are socially constructed and, as such, require a social context to be fully understood. Even security issues at a personal level such as authentication and trust in system reliability rely on social norms. Ultimately this paper highlights the changing shift in organizational security from an authoritarian 'enemy within' approach towards a more user centred one. However, it is through understanding how ‘communities of practice’ bridge the gap between the user and organisation that designers and policy makers will develop truly effective security.

Security and privacy do not only need to be addressed at the organizational level; communities should also be considered by privacy designers to have their own identity which requires protective mechanisms and policies. By interweaving approaches to individual and community privacy, computers can more accurately represent the norms and social practices that exist in the world today. Ultimately, we live and work both as individuals and as part of communities, within organizations and society as a whole. Our understanding and acceptance of the world around us is couched within negotiated meaning of those contexts. Security needs to support users in seeing and negotiating safely on those terms within technologically mediated systems.

7. ACKNOWLEDGEMENTS

This work has been funded by ESRC (grant RES-355-25-0032). We are grateful to all participants in the study for their contributions, and to the hospital authorities for their cooperation.

8. REFERENCES

Ackerman, M. S., 2004. Privacy in invasive environments: next generation labeling protocols. Personal and Ubiquitous Computing, Springer. (8). 430–439

Ackerman, M. S. and Cranor, L. F., 1999 Privacy Critics: UI Components to Safeguard Users Privacy. Proceedings of the ACM conference on Human Factors in Computing Systems (CHI’99). 258-259

Ackerman, M. S., Darrell, T. and Weitzner, D., 2001. Privacy in Context. Human Computer Interaction. 16.2/4. 167-176.

Adams, A., 1999a. Users’ perceptions of privacy in multimedia communication. Proceedings of CHI’ 99, Pittsburgh. ACM Press. 53-54

Adams, A., 1999b. The Implications of Users’ Privacy Perceptions on Communication and Information Privacy Policies. Proceedings of Telecommunications Policy Research Conference. Wash. DC. TPRC Press. 65-67

Adams, A., 2000. Multimedia information changes the whole privacy ballgame. Proceedings of computers freedom and privacy 2000: challenging the assumptions. Toronto. **ACM** Press. 25 - 32.

Adams, A. and Blandford, A., 2004. The unseen and unacceptable face of digital libraries. Journal of Digital Libraries. Springer, Heidelberg. 4 (2). 71-81.

Adams, A & Blandford, A., In Press. Organizational communication and awareness: a novel solution” Health Informatics Journal. Sage Press.

Adams, A., Blandford, A. and Lunt, P., In Press. Social empowerment and exclusion: a case study on digital libraries. ACM Transactions of computer human interaction (TOCHI) ACM Press.

Adams, A. and Sasse, M. A., 1999. The user is not the enemy. Communications of ACM. ACM Press (Dec. 1999) Vol. 42 (12). 40 – 46

Adams, A and Sasse, M. A., 2001. Privacy in multimedia communications: protecting users not just data. Proceedings of HCI’01, Lille. Springer. 49 – 64

Agre, P.E.,1997. Beyond the Mirror World: Privacy and the representational Practices of Computing, in: Agre, P. E and Rotenberg, M. (eds.) Technology and Privacy the New Landscape. MIT Press, Mass. 29-62

Altman, I., 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding. Monterey, CA: Brooks/Cole Pub. Co., Inc. Springer-Verlag

Augoustinos, M and Walker, I., 1995. Social Cognition: An integrated introduction. Sage Publications: London.

Bellotti, V., 1996. What You Don’t Know Can Hurt You: Privacy in Collaborative Computing, in Proceedings of HCI’96. Springer. 241 – 261.

Bellotti, V. and Sellen, A., 1993. Designing of privacy in Ubiquitous computing environments, in proceedings of ECSCW’93, the 3rd European Conference on Computer-Supported Co-operative Work”, Kluwer (Academic Press), 77-92.

Bennett, C., 1992. Regulating Privacy. Cornell University Press. London

Bennett, C., 1997. Convergence revisited: towards a global policy for the protection of personal data, in Agre, P. E and Rotenberg, M., (eds.) Technology and Privacy the New Landscape MIT Press, Mass 99-123.

Brin, D., 1998. The Transparent Society. Addison-Wesley, Reading, Pa

Clarke, R., 1999. Internet privacy concerns confirm the case for intervention. Communications of ACM. (Feb. 1999). 60 – 67

Cicourel, A.V., 1990. The Integration of Distributed Knowledge in Collaborative Medical diagnosis. In: J. Galegher, R.E. Draut and C. Egido (Eds.) Intellectual Teamwork. Hillsdale, NJ: Lawrence Erlbaum Associates. 221-242.

Covi, L. and Kling, R. 1997. Organisational dimensions of effective digital library use: Closed rational and open natural systems model. In Kiesler, S (Ed.) *Culture of the Internet.* Lawrence Erlbaum Associates, New Jersey. 343-360

Cranor, L. F., 1998. The platform for privacy preferences. Communications of ACM. ACM Press Vol. 42 (2). 48 – 55

Cranor, L. F., 2003. Web privacy with P3P. O'Reilly, Cambridge, Massachusetts.

Davies, S., 1997. Re-engineering the right to privacy. In: Agre, P. E and Rotenberg, M., (eds.) Technology and Privacy the New Landscape. MIT Press, Mass. 143-166

Dourish, P., 1993. Culture and Control in a Media Space. Proceedings of ECSCW'93, Kluwer (Academic Press). 125 – 137.

Goffman, E., 1969. The presentation of self in everyday life. Penguin press, London.

Harper, R. H. R., 1992. Looking at ourselves: An examination of the social organisation of Two Research Laboratories. Proceedings of the conference on Computer-Supported Cooperative Work (CSCW'92) ACM Press. 330-337.

Harrison, G. S., 1991. The Winchester experience with the TDS hospital information system. British Journal of Urology. 67.5, 532-535.

Harrison, R. and Dourish, P., 1996. Re-Place-ing Space: The Roles of Place and Space in Collaborative Systems. In Proceedings of the Conference on Computer-Supported Cooperative Work (CSCW'96), ACM Press. 67-76.

Heathfield, H., 1999. The rise and fall of expert systems in medicine. Expert Systems, Vol. 16, No.3. 183 – 188.

Hong, J., 2004. An artchitecture for privacy-sensitive ubiquitous computing. Proceedings of 2nd International conference on Mobile systems, applications and services (MobiSys, 2004). 177-189.

Jackson, L., Eye, A., Barbatsis, G., Biocca, F., Zhao, Y. and Fitzgerald, H., 2003. Internet Attitudes and Internet use: some surprising findings from the HomeNetToo project*1. International Journal of Human-Computer Studies. V.59 (3) 355-382.

Kling, R., 1996. Information Technologies and the shifting balance between privacy and social control. In: Kling. R., (eds.) Computers and Conroversy: value conflicts and social choices. Academic Press. London

Lave, J. and Wenger, E., 1991. Situated learning: legitimate peripheral participation. Cambridge: Cambridge University Press.

Lederer, S., Mankoff, J, and Dey. A., 2003. Who wants to know what when: Privacy preference determinants in ubiquitous computing. Proceedings of the ACM conference on Human Factors in Computing Systems (CHI'03), ACM Press. 724-725

Lederer, S. Dey. A and Mankoff, J., 2002. Everyday Privacy in Ubiquitous Computing Environments. Presented at the workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, Conference on Ubiquitous Computing, Ubicomp 2002.

Lederer, S., Hong, J., Dey, A. and Landay. J., 2004. Personal Privacy through Understanding and Action: Five Pitfalls for Designers. In Personal and Ubiquitous Computing 8(6), November 2004. 440 – 454.

Levy, S., Bradley, M. J. M., Swanston, M. T. and Wilson, S., 2001. Power as a concept in the evaluation of telehealth. In: Rushmer, R. K., Davies, H. T. O., Tavakoli, M. and Malek, M. (eds). Organisation development in health care: Strategies issues in health care management (2001) Ashgate Publishing Ltd.

Millen, D. R., Fontaine, M. A and Muller M. J., 2002. Understanding the benefit and costs of communities of practice. In Communications of the ACM. Vol. 45 (4), 69-73

Morgan, G.,1991. Images of organization. London: Sage.

Palen, L. and Dourish, P., 2003. Unpacking privacy for a networked world. Proceedings of the ACM conference on Human Factors in Computing Systems (CHI'03). ACM Press. 129 -136

Parker, D. B., 1992. Restating the foundation of information security. In: Gable, G. G. and Caelli, W.J., (eds.) IT Security: The Need for International Co-operation Elsevier Science Publishers, Holland.

Raab, C. and Bennet, C., 1998. Review of the Distribution of Privacy Risks: Who Needs Protection?. The information Society 14: Taylor and Francis. 263-274

Reidenberg, J., 1993. Rules of the road for global electronic highways: Merging the trade and technical paradigms. Harvard Journal of Law and Technology. 6. 287-305

Reddy, M. and Dourish, P., 2002. A finger on the Pulse: Temporal Rhythms and information seeking in medical work. In Proceedings of ACM CSCW'02. ACM Press. 344-353

Riegelsberger, J., Sasse, M. A. and McCarthy, J., 2003. Shiny happy people building trust/: photos on e-commerce websites and consumer trust. Proceedings of the ACM conference on Human Factors in Computing Systems (CHI'03), Short papers. ACM Press. 121-128.

Sandellowski, M. 1999. Culture, conceptive technology and nursing. International Journal of nursing studies, 36, (1999) 13-20

Schein, E., 1990. Organizational culture. American Psychologist, 45, 109-119.

Schneider, K. 7 Wagner, I., 1993. Constructing the Dossier Representatif: Computer-based information sharing in French hospitals. Computer Supported Cooperative Work, 1, 229-253

Schoeman, F. D., 1992. Privacy and Social Freedom. Cambridge university press. Cambridge

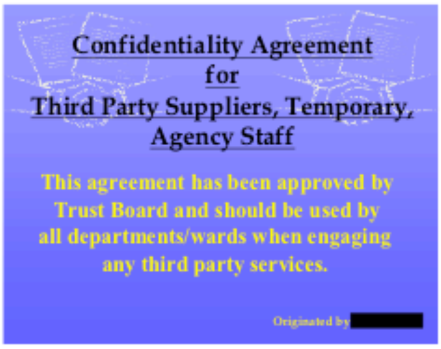
Strauss, A. and Corbin, J., 1990. Basics of qualitative research: grounded theory procedures and techniques. Sage, Newbury Park.

Symon, G., Long, K. and Ellis, J., 1996. The Coordination of work activities: co-operation and conflict in a hospital context. Computer supported cooperative work, 5,1. 1-3.

Wenger, E., 1999. Communities of practice: Learning, meaning and identity. Cambridge: Cambridge University Press.

Wacks, R., 1989. Personal Information: Privacy and the Law. Oxford Press. Clarendon

Whitten, A. and Tygar, J. D., 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Proceedings of the 9th USENIX Security Symposium: http://www.cs.cmu.edu/~alma/johnny.pdf

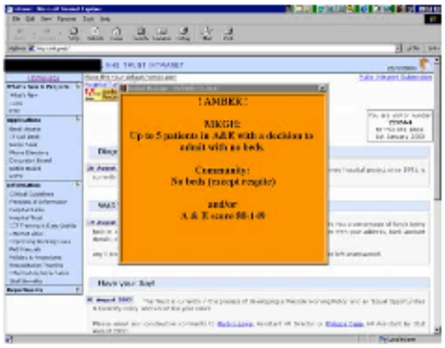


Confidentiality Agreement
for
Third Party Suppliers, Temporary, Agency Staff

This agreement has been approved by Trust Board and should be used by all departments/wards when engaging any third party services.

Originated by [redacted]

Figure 1. Privacy screen saver.



[redacted] NHS TRUST INTRANET

! AMBER !

MKGH:
Up to 5 patients in A&E with a decision to admit with no beds.

Community:
No beds (except respite)

and/or
A & E score 80-105

Figure 2. Alert traffic light screen.

	Ref .	Job	Status & Role	No.	Web-based information resources used
Provincial Hospital	St1	Clinicians, Nurses etc.	Nurses, Consultants, Managers, Library, IT & Security staff	20	Medline, the Cochrane library and the UK National electronic Library of Health (NeLH), Specialist web-sites, Department of Health web-site, Google to search the web.
Inner City Hospital	St2a	Nurses	Pre-Registration & Registered	36	(as above)
	St2b	Clinicians etc.	Doctors, Consultants, Surgeons, Allied Health Professional, managers & IT	37	(as above)

Table 1. Participant descriptive data

(Study reference numbers are included for reference in quotes used in the paper)

	Job	No.	% who raised security & privacy issues
STUDY 1: **Provincial Hospital**	Clinicians, nurses etc.	20	85%
STUDY 2: **Inner City Hospital**	Nurses	36	33%
	Clinicians etc.	37	62%
	Totals for study 2		
	Clinicians, nurses etc.	73	48%

Table 2. Percentage of Security / Privacy Issues within each context

STUDY 1: **Provincial Hospital Specific Issues**	**% of participants who highlighted this issue**	**STUDY 2:** **Inner City Hospital Specific Issues**	**% of participants who highlighted this issue**
Organizational security awareness	67%	Authentication as a barrier to work practices	38%
Trust in system reliability & security	58%	Authentication requirements	7%
Privacy and Confidentiality	42%	Security restricting valid activities	3%
Emergency security alerts	33%	Providing more access to personal information	1%

Table 3. Study specific security and privacy sub-issues