

Chapter 1: Introduction

Adoption of multimedia communications has vastly increased over the past decade and with the rapid advance of network and compression technology, this expansion can be expected to continue growing (Crowcroft et al., 1999). Applications for this technology include real time remote collaboration (e.g. videoconferencing, virtual reality), broadcasting of multimedia data on a global scale (e.g. multicast lectures, seminars and events on the Internet; Macedonia, & Brutzman, 1994) and digital libraries of recorded multimedia data. However, ubiquitous computing has global implications across domains and cultures. The increase in the provision of more varied data and ways of accessing it is not only leading to potential information utilisation benefits but also associated privacy risks.

As multimedia is a nebulous term that is vastly overused it is essential to clearly define this expression. Since multimedia communications rely on digital media the following definition has been applied for this research:

"...computer-controlled integration of text, graphics, still and moving images, animation, sounds and any other medium where every type of information can be represented, stored, transmitted, and processed digitally." (Fluckinger, 1995)

It is also important to understand the many interaction variations that can occur with this technology. Multimedia communications can vary between the style of interaction (synchronous or asynchronous) to the location (local or remote) and number of participants (from one-to-one, one-to-many and many-to-many). However, as Goffman (1981) highlights communication can still occur only in one direction (e.g. from speaker to hearer/s). With regard to privacy it is also vital to note the degree of involvement the system end-user has with the technology system as this could relate to their interaction awareness. This thesis therefore reviews communication at all levels of user and system interactivity (e.g. system interactive, system semi-interactive, system non-interactive).

It is often suggested that privacy is a basic human requirement (Schoeman, 1992). However, privacy, within technically mediated interactions (i.e. users interacting with technology to achieve goals), is a complex phenomenon, which varies across individuals, organisations and cultures. The process of defining this phenomenon is complicated further by different disciplines' research of this issue from different perspectives, using contrasting terminology and methods. Legal definitions attempt to define clearly *Private Information* or actions (Rubinfeld, 1989; Reinman, 1995). Psychologists seek to operationally define the phenomena for experimentation whilst computer scientists address users' privacy capabilities through system control and feedback. Although it is important to review all these perspectives and ensuing definitions, to provide a context for this investigation (see Chapter 2), the research reported in this thesis seeks to explore and define users' perceptions of privacy. To this end privacy will not be pre-operationally defined as it is suggested that this will reduce the researches' bias towards this phenomena. Taking this approach will provide the research with the flexibility to pursue any aspects of privacy that are defined by the users.

1.1 RESEARCH PROBLEM

As global multimedia communications supports interactions it also assists in the *freedom of information*. However, identifying the limits of users' acceptance of privacy risks is also important as perceived infringements of privacy may lead to the rejection of a communication technology thus decreasing its commercial viability.

Pivotal to the concept of privacy is a notion of the individual and their relationship with society (Wacks, 1989). For us to be private there must be a public environment to be private from. Privacy and thus being private can only be reviewed within that public context (Goffman, 1969; Agre, 1997¹). Privacy is therefore an important concept within social interactions and communications. Technology mediated communications also have related privacy implications, which are greatly increased within multimedia interactions. Multimedia environments can produce user perceptions of a relatively normal interaction whilst distorting the communication sphere and decreasing social cues so that natural assumptions are inaccurate. Multimedia communications also incorporate more complex data (with associated privacy risks) than other technically mediated interactions. Whereas a simple text communication will relay the basic information in a conversation, audio and video communicate further personally defining information that can be potentially more invasive. For example, an email may show that someone is upset about an issue, but the sound of a shaky voice and seeing their tears may reveal just how emotional they have become. This type of multimedia scenario may become invasive if the user did not want or know that this information was being transmitted.

Davies (1997) argues that there are many inalienable privacy rights which should never be disregarded when developing systems. Similarly, Bennett (1997) maintains that privacy experts understand potential privacy risks at a greater depth than users. Both of these arguments have directed privacy research and identification of privacy requirements in system development towards appraisals by privacy experts. However, privacy relies 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. Therefore identifying users' perceptions of privacy is an important element in both distinguishing what needs to be protected and how best to protect it. Empirical research into users' privacy perceptions, however, is very limited, especially within multimedia communications.

This thesis seeks to address these knowledge gaps by detailing users' perceptions of privacy within multimedia communications thus identifying the cause of potential privacy risks and how they can be addressed in the design, implementation and use of this technology. To this end three main research aims will direct this thesis:

1. To identify factors affecting users' perceptions of privacy within multimedia communications.

¹ As Agre (1997) points out information is not a commodity but strongly embedded in the way we live our lives.

2. To isolate factor relationships causing potential privacy invasions and potential solutions.
3. To verify a model of these factors and their relationships through further research and external expert evaluations.

1.2 RESEARCH SCOPE

The main objective of this research is to develop an understanding of the impact that user perceptions of privacy have on their attitudes to, and behaviour within, multimedia communication environments. Bellotti & Sellen (1993) point out that inadequate feedback and a lack of control for users can cause breakdowns in technology mediated interactions, and often lead to users rejecting the technology or using it in a less effective manner. This will then potentially effect the commercial viability of technological advances. This review also, therefore, aims to reflect any dynamic changes in technology that occur and their effects on users' perceptions and usability.

It is important to define the scope of this thesis so that the reader can identify limitations when applying the findings. Therefore, a detailed account of the research scope will be presented in three sections: (A) Users' (B) perceptions of privacy within (C) the domain of multimedia communications.

(A) Although users' cultural backgrounds may be key in shaping users' privacy perceptions this thesis will not review these broad and complex issues. A western (UK and US) privacy focus will be taken, as this research is limited to these participants by access issues.

As the users' technical experience has been noted as an important factor in privacy perceptions (Preece et al., 1994) this thesis will seek to compare both novice and expert user perceptions. Since the subject area is sensitive, capture of personalised details such as age, sex and occupation is deemed too sensitive for capture across all studies. However, as far as possible, a representative sample of the user population will be obtained for each study.

(B) This research aims to identify user privacy perceptions prior to, during and after a perceived invasion of privacy has occurred. This is to identify key factors that guide perceived invasions of privacy and processes that induce this occurrence.

Although users' perceptions of legislation, policy and standards or privacy mechanisms may be indirectly applicable to this thesis (users disregarding certain issues as they are – inaccurately – perceived to be secured by privacy legislation or privacy mechanisms) users' direct perceptions of these issues are outside its scope. In-direct issues will also not be a key focus here.

(C) Multimedia conferencing via IP multicast and Virtual Reality will both be reviewed within this research to increase the generalisation of results. Varying levels of system interaction (e.g interactive, semi-interactive and non-interactive) will also be reviewed since awareness and system controls are

argued to be key factors in privacy perceptions (Bellotti & Sellen, 1993). This will mean that for some studies system users may not be aware that they are relaying data.

For this research both reciprocal and non-reciprocal communication of data will be reviewed for network scenarios of ; one-to-one, one-to-many and many-to-many. These types of technical mediated interactions will be used as a medium for information exchange tasks. This refers to the main rationale behind the introduction of the technology but does not refer to the users' awareness of this rationale. As there is a clear distinction between business (including educational) and residential multimedia communication needs and user perceptions (Kraut & Fish, 1997) only the former will be reviewed within this thesis (see Section 3.2). Two types of information exchange tasks will be reviewed:

1. general usage (conferencing etc.);
2. specific usage (learning tool – tutorials, meetings, awareness technology etc.).

Finally users' perceptions of data types (audio, video, animation, graphics) will be briefly reviewed for potential privacy effects. However, an in-depth appraisal of these issues will not be undertaken.

1.3 RESEARCH APPROACH

Privacy within multimedia communications should consider both the human and computer aspects of the subject. Previous research has addressed this subject from the perspective of specific disciplines and yet current system usage relies on both the user and computer interacting. Since this research topic is clearly interdisciplinary it is appropriate that the thesis approach should reflect this. As such the overall research approach for this thesis will be a Human Computer Interaction (HCI) approach as a design science, which is scientifically grounded using Grounded Theory (Strauss & Corbin, 1990). This thesis will, therefore, start by establishing existing knowledge of the phenomenon under investigation both in HCI and relevant disciplines.

Grounded Theory is used by this research as the governing methodology and guidance behind the theory building process (see Section 4.2). This thesis aims to aid in the design of applications which do not invade users' privacy for their expected context of use and is to be applied according to grounded design type principles (Cockton, 1999; Clarke & Cockton, 1999). It is important, however, that an emphasis is placed on users' perceptions within the social context rather than assuming that only individual differences govern privacy issues (see Section 2.3). The social context, although complex, is of particular importance as peer pressure, organisational and social norms have strong impacts on this socially dependent phenomenon. If these factors are not considered then any findings would be inadequate for designers and the effectiveness of their privacy designs could be confounded by the specifics of implementation situation. A review of the different traditional HCI approaches, not taken by this research, and their limitations can be found in Section 4.1 (in more detail in Sasse, 1997). This Chapter also highlights the placement of qualitative research within the HCI paradigm.

An empirical approach will be taken for collecting both qualitative and quantitative data to develop an explanatory model of users' perceptions of privacy and processes that influence it. However, as the nature of the phenomenon under investigation is both complex and sensitive, and there is little previous knowledge, many traditional HCI methodologies would be inappropriate (although some appropriate HCI methods are used e.g participatory design exercise, questionnaires, expert walkthroughs). Most of the data will also be qualitative in nature to aid in dealing with the complexity of the issue. A Grounded Theory research framework (Strauss & Corbin, 1990) will, therefore, be used to develop theories and confirm findings (see Chapter 4).

The subsequent model developed will be descriptive and explanatory in its origins (with some predictive elements from quantitative data sources). However with the use of Grounded Theory it should be generalisable enough to provide privacy guidance for system designers and technology deployers with similar situations and applications.

1.4 THESIS STRUCTURE

Chapter 2: The first Chapter of this thesis proper reviews the interdisciplinary literature from the domains of Psychology, Sociology, Philosophy, Political Science and Computer Science which have examined privacy and its connections with computer technology. Part 1 provides a backdrop for privacy from a high level perspective reviewing the different terms and approaches to this field of study.

Chapter 3: Although there has been little detailed empirical research on users' perceptions of privacy within multimedia communications, there have been a number of application-specific or anecdotal studies, which this Chapter reviews. A review of privacy is made within the following multimedia communication systems and applications:

- Videoconferencing
- Awareness technologies (portholes, active badges etc.)
- Virtual Reality
- Multicast & Conference multicasts

The Chapter concludes with a summary of the gaps within the knowledge base, which this thesis seeks to fulfil.

Chapter 4: This Chapter completes the background Part 1 with a chronicle of Grounded Theory. Arguments behind the thesis methodological position are detailed. Finally a summary of the various methods (qualitative and quantitative) used for each stage of the research and why these different approaches were appropriate is also provided.

Chapter 5: The thesis studies are detailed in three Chapters of Part 2. The initial results, which helped define prominent privacy factors within the model, are presented in Chapter 5. A study of passwords (study 1: Section 5.1) within comparative organisations helped to establish the Information Sensitivity factor, which was later elaborated upon within the other environments. The longitudinal study of videoconferencing usage by novice users (study 2: Section 5.2) identified the Information Receiver and Information Usage factors and important sub-issues later verified within other environments. Finally the VR environment (study 3: Section 5.3) verified these factors whilst issues of anonymity, social norms and perceived control were also highlighted.

Chapter 6: The studies within Chapter 6 and 7 develop and verify the model whilst identifying the importance of process effects highlighted in the privacy invasion cycle. Study 4, which reviewed experts using conference multicast technology, specifically identified the concept of privacy threats and invasions as they were being realised by multimedia communication users.

Chapter 7: An opportunistic study of a multicast video application (Study 5) details users' privacy perceptions during and after many perceived it had been invaded. A critical boundary is identified within users' privacy invasion perceptions that produced an emotive rejection of the technology and those who instigated it.

Chapter 8: The study results are used at the beginning of Part 3 for theory building within Chapter 8 in the form of the privacy invasion cycle and a model of users' multimedia communications privacy perceptions. This Chapter continually relates how the privacy model can solve potential privacy invasion cycle problems by 1) identifying the specific problems then 2) identifying what assumptions are inaccurate and finally 3) identifying whether feedback, more control or less control is required to solve these problems.

Chapter 9:

The model is evaluated, in Chapter 9, by detailing and reviewing expert walkthroughs from the perspective of Political Science, Multimedia communications and Security. A review is also made of these evaluations with regard to this thesis.

Chapter 10:

Chapter 10 concludes Part 3 by detailing what these findings mean to multimedia communication research and developments in the future. It also relays the limitations of current privacy approaches identified by this thesis's research (Studies 1-5).

1.4.1 Terms and typography

As an HCI perspective will be taken terms such as User will be used with an HCI definition as the system end-user. A different *typography* is used throughout the rest of the thesis to highlight terms that have been identified and used in a specific way by the author i.e. specific privacy model terms.

Within this domain authors use the terms data and information interchangeably while meaning different things. Although the concepts of data and information are closely linked, they denote different aspects of the same phenomenon. However this debate will not be reviewed since this thesis is only evaluating users' perceptions of data thus information.

Throughout the thesis a Grounded Theory analysis is presented of how the model develops. Every relevant section or sub-section is followed by a summary of which model factors are substantiated by that section. Each Chapter preceding the model is concluded with a summary of model contributions, gaps and further developments required.

1.5 THESIS CONTRIBUTIONS

There is an extensive amount of research from various disciplines (sociology, political science, philosophy etc.) that reviews privacy. Similarly there is much multimedia communication research, some of which evaluates privacy mechanisms. However, as pointed out in Section 1.1, there is little research into users' perceptions of privacy within multimedia communications. What little research that exists is either anecdotal in its origins or, if empirical, does not review the subject in great depth. As also detailed in Section 1.1 there is a critical need for this knowledge gap to be filled so that multimedia applications are not rejected through perceived privacy invasions. This thesis will therefore present a theory of the processes behind privacy invasions within multimedia communications. A model of what guides users' perceptions of privacy within multimedia communications will also be provided. It is argued that multimedia designers, researchers and implementers will be able to use these findings to develop and implement systems which reduce potential privacy invasions. The thesis findings will therefore make the following contributions:

1. Provide a fuller understanding of users' perceptions of privacy within multimedia communications.
2. Detail an account of specific privacy invasions and potential solutions within various multimedia environments.
3. Develop a model and theory that will aid in designing appropriate privacy mechanisms, policy designs and implementation.
4. Identify areas for further privacy research within multimedia communications.

Chapter 2: Privacy Background

As privacy is an interdisciplinary issue the background Part 1 (see Chapters 2, 3 and 4) reviews privacy sources from: Psychology, Sociology, Philosophy, Law and Computer Science to identify their relevance to Human Computer Interaction (HCI). These Chapters will also assess the applicability, within HCI, of privacy issues as social limitations which, if breached, produce reduced user performance and increased resentment.

This Chapter (see Diagram 2.1) initially reviews these issues from the abstract human interaction level (see Section 2.2). How we communicate and thus interact relies on many socially dependent factors. Arguments from various disciplines (as mentioned above) are reviewed which look at how technology interacts with natural social factors and can distort human interactions. These issues are examined together with how technology, as a broad concept, may be affecting privacy.

As privacy is a complex phenomenon this Chapter (see Section 2.2) proceeds to analyse how different disciplines define it. Initially, privacy and its invasion were considered, primarily within the legal domain centring on the concept of *Personal Information*. However, with the increased importance of computerised data, a more practical approach has been argued for, with increased user privacy controls (Bellotti & Sellen, 1993). Finally, as privacy relies on how it is perceived, a brief analysis of how users define privacy is presented.

Since a principle aim of this thesis is to identify privacy issues as social limitations this Chapter (see Section 2.3) also highlights various arguments about potential causes of privacy invasions within technology mediated interactions. Various theoretical and empirical perspectives are reviewed concerning the perceived sensitivity of the data transmitted, who receives it and what it is used for. Finally a number of different viewpoints are assessed with regard to the impacts of social and organisational issues on privacy invasion.

In concluding this Chapter (see Section 2.4) an examination is made of the different approaches that have been taken towards privacy invasion. One major perspective is the political science one although, with the rise of computerisation, the importance of the technical approach has increased. However, over recent years there has been a leaning towards manipulating users' perceptions of privacy with the use of a *semantic cueing mechanism* approach (CFP, 1997). Semantic cueing mechanisms (e.g trust badges, opting-in vs. opting-out, P3P) seek to increase the user's perception of control by cueing positive privacy perceptions (see Sub-section 2.4.2). Finally, a review of the importance of users' perceptions in privacy invasion is assessed. Ultimately it is users not privacy advocates or lawyers who know if their privacy has been invaded. However, there is insufficient research specifically into how users perceive privacy.

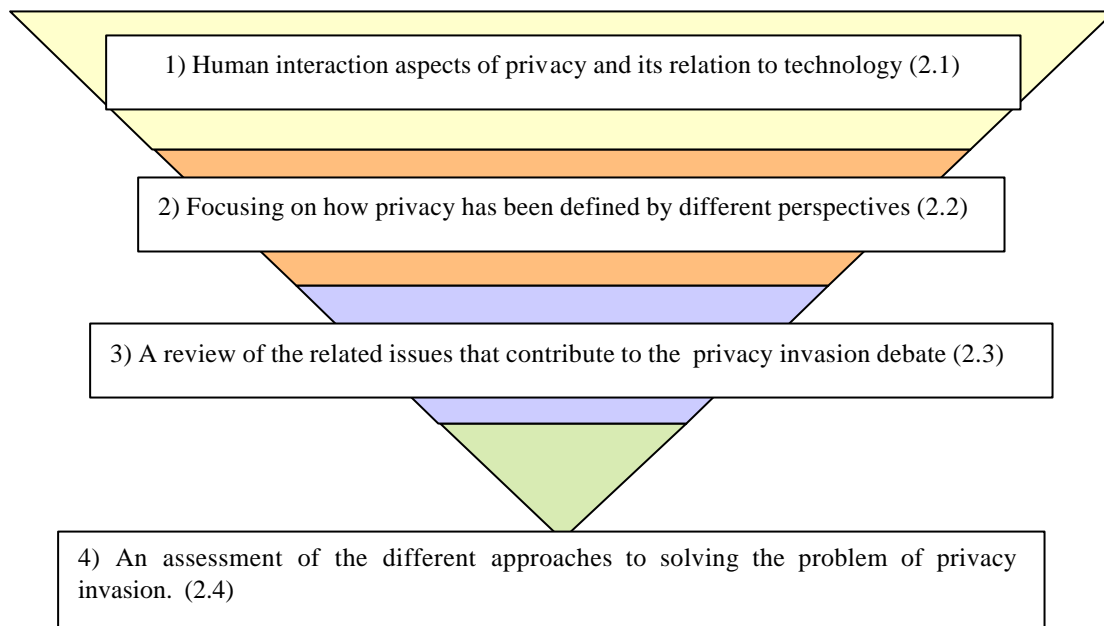


Diagram 2.1: Focus of Chapter 2

2.1 SOCIAL INTERACTION, PRIVACY AND TECHNOLOGY

Throughout our lives we develop *mental models* (internalised mental representations) of the world and our interactions. Mental representations contain both procedures and conceptual structures based on incoming information being associated with already existing knowledge (Johnson-Laird, 1983). These mental models play a central and unifying role in our conceptions of the world and enable us to predict and interact with it. You may have a mental model of a restaurant; what is expected to be found (e.g. plates, food, tables, cutlery), to occur (e.g. ordering food, eating food, paying for that food) and how you should behave there (e.g. etiquette - table manners, tipping etc). However, as Harrison & Dourish (1996) point out, our mental models cannot be purely cognitive as they develop within cultures where learning them is part of our assimilation and socialisation. These mental models are, therefore, affected by previous experiences that are often couched within cultural contexts (e.g. US tipping culture, Greek plate throwing etc). As mental models are central in our interaction perceptions, it is not unusual that this concept is referred to within the discipline of HCI. Yet, it is often difficult to relate this knowledge back to specific system design recommendations (Tognazzini, 1991). This could be due, as Norman (1983) points out, to mental models *not* being scientifically based but instead incomplete, unstable and often superstitiously based. However, what is frequently overlooked is that our perceptions of the

situation (place) are important in guiding our behaviours and thus our mental models (Harrison & Dourish, 1996). Both Goffman (1969) and Giddens (1984) suggest that our behaviours are framed within a specific situation. Situations are defined by both the physical aspects of the place and the knowledge and expectations of others present there. Table 2.1 shows that although both situations take place in the same location (a sports hall) the activities are different and thus the social acceptability of the same user actions are completely different.





	SITUATION A	Acceptability	SITUATION B	Acceptability
Location: Sports Hall	Sports Club		Flower arranging club	
User actions (a massage)				

Table 2.1: Social acceptability of actions for different situations

We all assume that in many situations we know what is acceptable and unacceptable behaviour (e.g. acceptable to clap at the end of a theatre performance but not at the end of a funeral service). However, these codes change within different cultures and these cultures can vary between organisations, cities or countries. Although the divides of what is acceptable or unacceptable can change between societies most people *within* those societies know where the boundaries are. Therefore those who breach those social barriers are usually fully aware they are doing so (Goffman, 1969). These changes in social codes can relate strongly to many multimedia communication systems as the Internet crosses many organisational, country and cultural boundaries. In the real world moving between different cultures can be difficult but the human ability to adapt enables many of us travelling between different cultures to learn what is acceptable or unacceptable by social cues from others within that culture. What is of vital importance, therefore, is for us to receive feedback of what is acceptable and unacceptable within that culture for that situation (Goffman, 1969; Giddens, 1984). This allows non-members of a community the ability to assess whether they can adjust to the cultural changes or not. Social cues, norms and pressure are therefore exerted to produce informed knowledge of acceptable and unacceptable behaviours (Goffman, 1969). What is accepted as social or anti-social behaviours, however, not only varies between cultures but between different situations and contexts. This allows us to retain some degree of privacy within certain contexts where we can have the freedom to express ourselves and our individuality free from social censorship (Schoeman, 1992). However, the privacy

distinction between some situations is more obvious (e.g. a department store changing room vs. a bedroom) than between others (e.g. a small open plan office vs. a common room). Within *virtual spaces* (“*collaborative computational environments*”) these privacy distinctions become even more blurred (Harrison and Dourish, 1996).

Contextual cues can allow us to judge the degree of privacy afforded by different situations. Goffman (1969) highlights the importance of these contextual cues with the example of the *front* and *back* sections of society (front and back entrance to a house, different sections within a house or city) which are often physically presented (e.g. restaurant front entrance grand, back entrance coarse) with visual cues. Goffman (1969) also notes how some back street behaviours are deemed as inappropriate on the main street and vice-versa. Physical cues for each situation can act as an added cue to appropriate behaviour within that situation. However, both Goffman (1969) and Giddens (1984) argue that mere physical cues are pointless without a shared understanding of the place within that community. It is important to add that multimedia environments have been noted as varying in the level of contextual cues which enable users to appropriately frame their interactive behaviour. (Harrison & Dourish, 1996). However, the privacy implications for these inadequacies within technically mediated interactions have yet to be highlighted. A public environment that implies by contextual cues that it is private is more likely to lead to an invasion of users’ privacy than one that clearly gives cues that this is a public situation.

Grounded Theory model building

This section partially supports the model factors:

User factor: mental models (Sub-section 8.3.1.1)

Information Sensitivity (IS): Public / private situation (Sub-section 8.3.2.2)

Information Usage (IU): Later IU – context (Sub-section 8.3.4.4) the importance of contextual cues is detailed (i.e. losing these cues could produce misinterpretations).

Context: Social groupings – social groups (Sub-section 8.3.5.4)

Context: Social groupings – social group outsiders (Sub-section 8.3.5.5)

Context: National and international – cultural norms (Sub-section 8.3.5.8)

the importance of context factors such as social groupings and cultural norms can change perceptions of what is acceptable or unacceptable with regard to privacy.

2.1.1 Social interactions and technology

Social interaction is complex and, although researched for centuries, much of the reasoning behind our social behaviours still eludes us. It is not surprising, then, that when we sought to devise a virtual world to interact with and through we should seek to replicate the real world rather than invent a new one (Agre, 1997; Laurel, 1993). As our social sphere is so complex it also is not surprising that this can often develop into a simplification of the world. However, because users equate mediated life with real life computer mediated interactions often trigger a wealth of socially determined responses, whether the

system designer's meant for them to occur or not (Reeves & Naas, 1996). These social responses are natural and intuitive, which means that, although they can be fought against by treating a computer as a simple object (i.e. computer mediated interactions without social connotations), we naturally tend towards such reactions.

There have been many accounts of virtual worlds being modelled on the real world. Agre (1997) presents a comprehensive review of the replication of reality by computer designers. The limitations of the *Mirror World* (Gelernter, 1991) approach when looking to devise privacy enhancing technologies are also presented. The mirroring of the real world in a computer format has been a guiding influence and sometimes a source of design flaws at all levels of computer system design (Agre, 1997). Neural nets are a source of architectural simulations of the brain while Virtual Reality has sought to simulate whole environments virtually. Within multimedia communications real world spatial metaphors are often used to assist and shape interactions (Harrison & Dourish, 1996). Interface design is also renowned for its use, sometimes detrimentally, of metaphors e.g. the *desktop metaphor* (Lakoff and Johnson, 1980; Laurel, 1993) is meant to aid users transfer their understanding of office filing, utensils etc. to similar interface scenarios. Even the language used within an interface can be based on metaphors and has been found to affect the mental model developed by the user (Clarke & Sasse, 1997). Emotive relationships have also been noted as associated with linguistic metaphors². The advantages of this approach in system design are numerous but two important benefits for the user are an:

- Increased sense of familiarity and thus comfort with the environment.
- Increased ease in the assimilation and learning of a familiar environment.

However, there are problems within HCI with this approach namely that:

- Confusion and disorientation will occur if there are elements of the virtual world that do not match the real world.
- Advantageous elements of the virtual world may be missed, because they do not fit the users' (or designers) mental model of the real world metaphor.

This thesis argues that the confusion and disorientation experienced by many users, within Internet and multimedia communication environments, could be due to a lack of shared social and physical cues (see Section 2.1). The Internet, in particular, covers most continents and thus many cultures and yet it can isolate us from the very social cues that allow us to adapt our behaviours accordingly. Within the virtual world there are often no clear communities with cues of what is acceptable or unacceptable behaviour. The division between acceptable and unacceptable behaviour has a direct impact on privacy within virtual environments. Even within specified communities *context cues* are often lacking thus

not allowing us to accurately judge appropriate behaviours for different situations. This can lead to confusion regarding where the public or private divide occurs. Laurel (1993) notes that, as with theatre, the interface (i.e. the stage and its actors) is all the user sees or is interested in. This highlights the importance, for the user, of cues that are often missing in interface designs. Harrison and Dourish (1996) argue that it is the sense of place rather than the physicality of space that frames our behaviours. Many collaborative and communication environments are designed around replicating real world spaces through spatial metaphors. However, they highlight that these replications do not produce the socially constructed understanding of place we require for mediating our interactions. Ultimately, many cues can be relayed within a virtual format but much is often missed. Worse than a lack of cues, however, is the presentation of inaccurate cues. If we have an inaccurate mental model of a communication environment we are likely to inaccurately predict its behaviour or act inappropriately.

A simple replication of a real world scenario, which is not supported by the system, is a frequent cause of user misconceptions encountered by HCI professionals. There has subsequently been much research, within the HCI field, into users' mental models (Carroll & Olson, 1988; Norman 1983), developing systems around them (Norman, 1986; Clarke & Sasse, 1997) and specific metaphors that aid or hinder their development (Hutchins et al. 1986; Lakoff and Johnson, 1980; Norman 1983). Desktop metaphors are often presented as an example of how a user is encouraged in the misconception that they are acting directly upon entities (e.g documents, files) when they are only acting upon an interface that then interacts with the system (Johnson, 1987). This can lead to an inaccurate mental model of their actions and control within these environments. For example, a user could misconstrue that typing in a word processed document is saved continually as a real world document is changed immediately that we write or type on it. This could lead to a word processing mental model that does not contain the action of saving a document.

Ultimately it is vital for users to understand that the virtual world is *not* a simple replica of the real world and thus assumptions on that basis should not be made. I do not argue that we should remake the virtual world removed from the real world, as this would be impossible. Every perception we have and every action we take is couched within our experiences and understanding of the social world around us (Goffman, 1969; Giddens, 1984). However, users must understand, in order to safeguard their privacy, that many everyday assumptions we make to help us navigate our everyday life are often not supported and are inaccurate within the virtual world (see Diagram 2.2).

² Linguistic metaphors are often used in every day conversations. An argument, for example, is often referred to as a battle with sides, defenders, attackers where an argument can be 'shot down'. Emotive associations with this

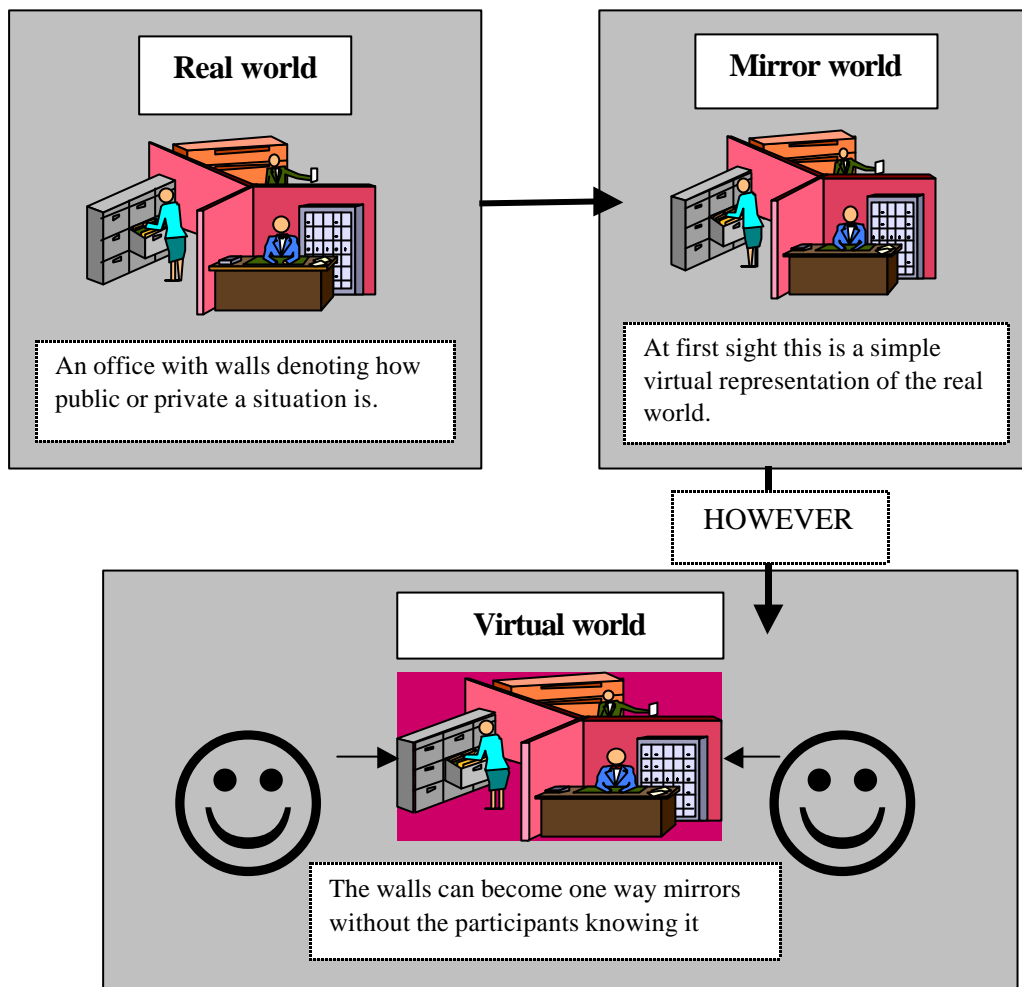


Diagram 2.2: Translation of real world situations as assumed by users (mirror world) and in reality (virtual world).

It has been argued that privacy invasion is merely indicative of an information society (Krull, 1995). Technology itself can increase potential privacy invasions because of the inaccurate assumed privacy levels of certain applications. Although socially rich responses may be replicated within virtual worlds differences between the two worlds can make the interaction more complex and potentially dangerous with regard to privacy invasion. Not only are environments replicated, but also real world relationships can be replicated by the way we interact with the technology. Reeves and Naas (1996) suggest that our interactions with technology are determined by a human predisposition to divide things simply into two categories:

1. human-like with rich social behaviours; and
2. physical objects without rich social behaviours.

When using technology as a media for social interactions, they argue that we react to the technology as the former (1) rather than the latter (2). This argument is substantiated by studies they have conducted

metaphor also exist. To lose an argument is to feel defeated and bad. (Lakoff and Johnson, 1980)

into relationships between users and technology. Politeness protocols (Reeves & Naas, 1996) have been found to cause people to be more positive, and less honest, about someone to their face than to a 2nd person. Participants were found to respond unconsciously (contrary to respondents' conscious reports) in the same way when interacting with computers. However, this thesis proposes that privacy problems can arise when the technology is reacted to as human-like when it does not retain the expected social norms for social interactions. Karabenick & Knapp (1988) looked at tasks where students who failed to identify concepts in a task were allowed to seek help from a computer or another person. The proportion of those seeking help was significantly greater when the source of help was the computer rather than another person. This was identified as the perceived privacy and freedom associated with the technology. I argue that it is this perception that could be manipulated (intentionally or unintentionally) in certain contexts unbeknownst to the user.

Grounded Theory model building

This section partially supports the model factors:

User factor: mental models (Sub-section 8.3.1.1)

Information Sensitivity (IS): Public / private situation (Sub-section 8.3.2.2)

Context: Technology – interface issues (Sub-section 8.3.5.2) interface design issues, such as metaphors, can impact on perceptions of the interaction.

Context: Technology – presence (Sub-section 8.3.5.3) poor social cues and unconscious relationships with the technology can effect interactions.

2.1.2 Technology and privacy

Privacy has often been suggested as a basic human requirement. The U.S. Supreme Court ruled that privacy is a more fundamental right than any of those stated in the Bill of Rights (Schoeman, 1992). With an increase in computer monitoring and external information control, privacy invasions have even been linked to stress (Aiello & Shao, 1993; O'Neill & Carayon, 1993). The importance of this factor can also have far reaching economic repercussions for developing technologies as Cowan (1983) identified when most people, on a budget, put privacy and autonomy above technical efficacy and public interest.

Privacy can be enhanced by different means (i.e. physical or technical means) and is culturally bound to be sought in different ways. However, ubiquitous computing has global implications across domains and cultures. This is reflected by the numerous articles defending people's privacy from computerised record systems as opposed to the lack of papers defending the decrease in privacy to aid private profit or police protection (Kling, 1996; Reinman 1995). However, with the increasing availability of varied data and applications, which enable access to, and utilisation of such data the *privacy risks* associated are greatly increasing (Bellotti, 1996; Neumann, 1995; Smith, 1993). Kling (1996) suggests that over the past 30 years there has been an increased popularity in the opinion that computerisation has

decreased people's privacy. Computerisation, however, is not the only culprit in people's perceptions of decreased privacy; slow-to-react organisations have been noted as playing a key role in this decline. Organisations that develop privacy policies retrospectively after an external threat has occurred produce policies that have been outgrown by changes in either society or the organisation's activities (Smith 1993).

When reviewing privacy in detail its true complexity is revealed. In one study it was identified that, although 80% of Americans said the news media "*often invade people's privacy*" only 41% stated journalists are too aggressive in reporting the news (USA Today, 1997). Legislative developments have not untangled this complexity. Over the last 30 years U.S courts have increasingly ruled that personal records belong to an organisation and access cannot be restricted by the person in question (Kling, 1996). Ultimately computer system designers and policy makers have a complicated job trying to weigh up the importance of privacy against the call for freedom from censorship (James Boyle, 1997).

Grounded Theory model building

This section partially supports the model factors:

Information Usage (IU): Later IU – awareness (Sub-section 8.3.4.2) ubiquitous computing increases the information available with conflicting ownership issues affecting users awareness of what is captured and the information is used for.

2.2 DEFINING PRIVACY

Broadly, privacy can be defined as the right to be left alone when desired (Kling, 1996; Reinman 1995) which can be enhanced by different means: behaviour, words, and body language; space (a large house with ample grounds); security measures (locks and alarms); and legislative measures. Privacy is also regarded and sought differently throughout the world. Americans create physical barriers, whilst arguably the English specialise more in psychological barriers (Ornstein and Cartensen, 1991). The Japanese developed the movable wall to make space multi-functional while preserving situational privacy (Hall, 1969).

2.2.1 Legal definition

Reinman (1995) argues that, for there to be a right to privacy, private information or actions must be clearly defined. To achieve this, various attempts have been made to define privacy within legal terms. Legal definitions are, however, often vague and inappropriate for the peculiar nature of computing environments where the potential for privacy invasions is often unimaginable, let alone definable. Nevertheless, it is useful to highlight these legal definitions, as it is often clear to see how, although often inappropriately, they have directed research into privacy. Smith (1993) defines privacy as a condition of limited access to identifiable data about individuals. Rubinfeld (1989) also suggests that two basic types of privacy exist: decisions made about one's body and the secrecy of certain data. He

suggests that the secrecy of information is one of the common characteristics of privacy. However, as with the legislation these definitions do not clearly identify any variations, which may effect users' perceptions of privacy. In tort law there are four categories of individual protection:

1. intrusion upon a person's seclusion, solitude, or private affairs;
2. public disclosure of private embarrassing facts;
3. public disclosure of a person in a false light;
4. appropriation of another's name, image, or other aspect of identity, for one's advantage or profit, without that person's consent.

However, it is argued by this author that, as many of these categories are hard to define with regard to computer privacy protection, legal definitions are often reduced to those relating to *Personal Information* (see Diagram 2.3).

Grounded Theory model building

This section partially supports the model factors:

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

Personal information often relates to *primary information*(e.g. private facts disclosed)

2.2.2 Personal Information

Many privacy accounts often make a simple binary private or not private distinction by defining privacy with regard to *Personal Information*. As multimedia communication deals with complex data in a new way the current *Personal Information* policy paradigm must be reviewed to assess its appropriateness within this domain. The concept of *Personal Information* is a confusing term, which although widely used, is not often defined. Wacks (1989), however, in his book '*Personal Information: Privacy and the Law*' provides a clear definition:

"Personal Information consists of those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation." (P.26)

Two points should be highlighted from this definition; firstly that it is the individual's perception of what is intimate or sensitive that is presented as important, secondly that the information referred to 'relates to the individual'. However, a review of legal definitions (Raab,1998; Bennett, 1997) illustrates that as computers and thus policy making issues become more complex this has often been simplified (see Diagram 2.3) to:

- 1) experts' perceptions (not the individuals' perception) of what is sensitive to the individual;
- 2) defining data that is personally identifiable as the most sensitive (Bennet, 1992; Agre, 1997).

The simplification of complex psychosocial factors into the concept of *personal information* and then its simplification into two factors (see diagram 2.3) is a data-centric approach. This abridged perspective has probably developed because it supports uncomplicated privacy policy and legislation development.

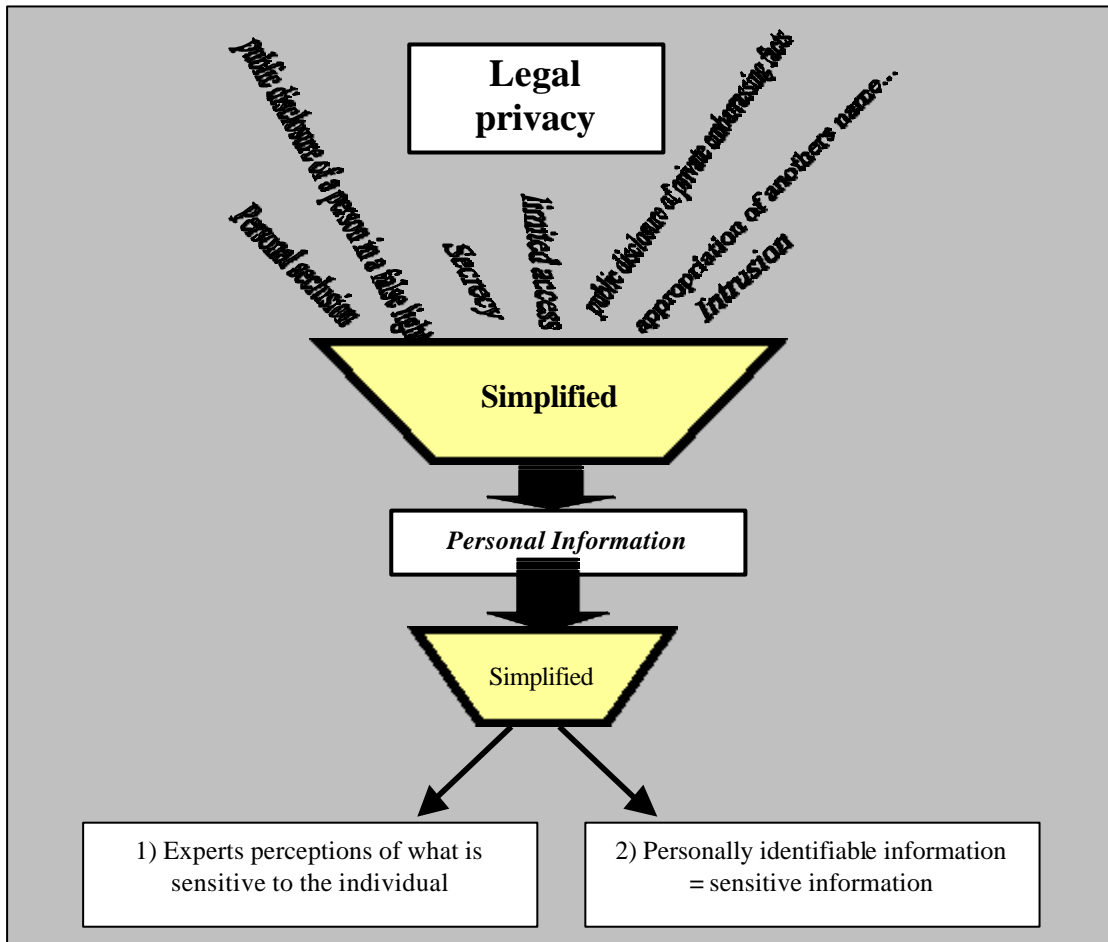


Diagram 2.3: The limitations of computer privacy definitions

The problem with many definitions of Personal Information is that they concentrate on the data itself rather than how it is perceived (Davies, 1997). It must be remembered that pivotal to the privacy concept is a notion of the individual and his or her relationship with society (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, 1997³).

Grounded Theory model building

This section partially supports the model factors:

Information Sensitivity: Judgement (Sub-section 8.3.2.1) the sensitivity of the information relates to users perceptions / judgements of it not an experts.

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

2.2.3 Practical definitions

Over the past decade, with the increased importance of computerisation, there has been a move to define privacy in more detail, especially with reference to its practical applicability. However, the term privacy has been noted as too restrictively defined by security specialists and computer scientists, especially in the United States (Clarke, 1997). These definitions refer only to the security of data against various risks (e.g data accessed or modified by unauthorised persons) or more specifically only to the security of data during transmission (Adams et al, 1997; Adams & Sasse, 1999c). It must be noted, though, that these aspects present only a small fraction of the considerations within the field of privacy which should be reflected by its definition.

Stone et al. (1983) suggested in their definition the importance for the “... *individual to personally control information about oneself*” (p.460). This was re-defined by Bellotti (1996) as one of the two common types of privacy definitions:

- Normative definition : (set of norms) aspects of a person’s nature and activity which are inherently private.
- Operational definition : (capabilities) access control or via the user’s control from feedback (see Section 3.4).

Schoeman’s (1992) distinction of a broad and a narrow conception of privacy emphasises this divide. The narrow end of the spectrum relates privacy exclusively to *Personal Information* and the extent to which others have access to it while the broader conception adopts issues such as anonymity and other forms of access. However, it has also been stated by Bellotti & Sellen (1993) that, to define privacy adequately, it must be understood that it is an unstable phenomena that varies according to context, users’ roles and societal / organisational norms, whilst privacy benefits can effect users’ overall perceptions. However, Bellotti & Sellen do not define what these factors mean. In addition, I would emphasise that the control and feedback approach to privacy also negates the importance of the trade-off that users make in certain situations. Rousseau suggested in 1762 that:

“Each person alienates, by the social compact, only that portion of his power, his goods, and his liberty whose use is of consequence to the community”. (p.38)

Davies (1997) presents an example of how within modern society users' privacy trade-offs have been successfully manipulated by organisations implementing technology (see Sub-section 2.3.4). To increase security camera usage within Britain, the public have been encouraged to believe in the overriding social benefits (greater good) of the technology outweighing their own personal privacy. However, this acceptable trade-off relies on user assumptions which, if inaccurate, can change the acceptability of the scenario. This clearly suggests the importance of contextual issues in all privacy

³ As Agre (1997) points out information is not a commodity but strongly embedded in the way we live our lives.

evaluations made by users. An operational definition of privacy should therefore consider this element of the phenomena.

Grounded Theory model building

This section partially supports the model factors:

Information Receiver (IR): Trade-off's group membership (Sub-section 8.3.3.5)

users can trade-off increased privacy risks against IR's membership to a specific social group with a valued role in the data.

2.2.4 User definitions

Privacy is often considered a right. Unfortunately, this concept gives the impression of an absolute standard such as legal rights or natural and moral rights (Clarke, 1997). Privacy is a complex phenomenon that defines who we are, by allowing for individual expression, and yet binds us into a society through social norms (Davies, 1997; Schoeman, 1992). Privacy is therefore not only an individual need, but is necessary for successful social interaction. Within real and virtual worlds the assumptions people make, and thus their perceptions, are often governed by social norms whether a computer system was designed to cater for them or not (Laurel, 1993; Reeves & Nass, 1996). There are two types of privacy norms (Schoeman, 1992):

1. Privacy that protects access to an individual in a specific context which is already privately regulated by *social norms*.
2. Privacy that protects access to an individual within a certain domain, but within that context allows for private expression and autonomy (private behaviour providing freedom of expression - private life, individuality etc.).

It is suggested by Schoeman (1992) that a relaxing of the norms for the latter (2), thus restricting intimate or personal opportunities, would be more of a violation than the former (1), that is already controlled by social norms. Therefore, an invasion of a person's freedom of expression free from social scrutiny would be more invasive than an invasion of private behaviour already controlled by social norms. Ultimately what is important to isolate from these concepts is that, as privacy relies on the individuals' perceptions of it, any definition should reflect this :

“Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations” (Clarke, 1997. p.2).

Grounded Theory model building

This section partially supports the model factors:

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

Context: Social groupings – social groups (Sub-section 8.3.5.4)

2.3 PRIVACY ISSUES

Past reviews of potential privacy invasions have concentrated on later *Information Usage* as a major cause of privacy invasions. Three main factors have been highlighted as important causes of privacy invasion (P.Hewitt, 1982):

- 1) Secrecy in data usage.
- 2) Inaccurate, irrelevant or out-dated data - secretly held.
- 3) Leaks of confidential data to unacceptable recipients.

All the privacy invasions detailed are due in part to the notion of secret data. One argument proposed to counteract these privacy problems is an increase in the *freedom of information*. This assertion is a pre-cursor to the proposition presented by Brin (1998) of the benefits of a transparent society. Brin, argues that new technology drives are irrepressible, and privacy safeguards futile. He maintains that privacy can only be secured by, instead, increasing the *freedom of information* for everyone. In short making everything public destroys the problems associated with secrecy. However, I propose that there are three important flaws to this approach. Firstly, for this approach to work there must be a utopian world where all information by everyone is free for access. 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*. It is idealistic to assume that this can be overturned for mere privacy reasons, there will always be the call for national and organisational security etc. The more *freedom of information*, it could be argued, increases the power of those who retain secret data, as these may be the missing pieces in the information puzzle. The second argument suggests that the call for *freedom of all information* is morally wrong because some information is inherently private in order for us to have our freedom of expression exempt from social scrutiny (Schoeman, 1992 : Sub-section 2.2.4). Finally the *transparent society* argument relies on secrecy being the main cause of privacy invasions. However, this assumes a limited nature of information denying its ever changing complexities. For example, information derived from the same data can change when interpreted by different people (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 cause of privacy invasions.

As computer technology has advanced so have the potential risks and the scope of issues involved. There are however, two major justifications that underpin the direction of further research (see Table 2.2). One argument that often arises in the privacy debate is that **some situations** will always cause people to be unhappy about their lack of privacy. The other argument is that **some people** will always feel that they require more privacy. However, this author argues that further research is required to identify the relevant importance of these two arguments.





	People		Situations	
Important differences	Person A	Person B	Situation A	Situation B
Privacy perceptions				
Further research	Individual differences		Contextual differences	

Table 2.2: Privacy issues a case of individual differences or contextual difference

Goffman (1969) highlights that when an individual takes part in an interaction there is an unknowing perception of the situation incorporating themselves. The presentation of the self within a perceived situation increases the privacy risks that are attached to interactions thus producing potential consequences at different levels of abstraction from the personal to the social. Subsequently, if an individual's perception of the situation is inaccurate then there are far reaching consequences. Changing perceptions of the situation can make previously established natural interactions inappropriate making individuals feel awkward, flustered etc. Social perceptions of ourselves may also be disrupted causing personal, social grouping and even organisational discreditation. Ultimately, it is an increased perceived freedom of self-expression and personal development, not restricted by social taboos, which retains highly charged emotional items that are the most intimate and private. It is users' perceptions of these situational factors that are vital to privacy invasion (Schoeman, 1992; Bellotti, 1997).

“At this stage we can better understand privacy by characterising the contexts in which it arises or is invoked as a concern.” (Schoeman, 1992. p.26)

However, Underwood & Moore (1981) have argued that behaviour not only varies between different situations, but that the degree of variation depends on the individual. People who have a high degree of *private self-consciousness* (who carefully monitor their own behaviour, even when others are not observing them) try to show consistent behaviour from situation to situation. Other people show more situational variability in behaviour. This relates to Schoeman's (1992) idea of certain behaviours being mediated by social norms although there is no clear identification here of which type of people are more or less affected. Taking these two arguments on board, I conclude that although peoples' reactions may vary in degrees certain contexts will invoke more concern than others. It is therefore important to identify the key issues producing contexts that can cause extreme privacy anxiety for some, if only slight anxiety for others.

Grounded Theory model building

This section partially supports the model factors:

User factor: user distinction (Sub-section 8.3.1.2) an interaction is reliant on shared understandings of the situation between the interaction participants.

Information Sensitivity: Judgement (Sub-section 8.3.2.1)

Information Sensitivity: Public / private situation (Sub-section 8.3.2.2)

Information Usage (IU): Current IU – task (Sub-section 8.3.4.1) perceptions of the situation and thus the task can effect perceptions of the information sensitivity.

Information Usage (IU): Later IU – context (Sub-section 8.3.4.4)

Context: Social groupings – social groups (Sub-section 8.3.5.4)

2.3.1 What information?

Data is increasingly being treated as property. The National Basketball Association (NBA) has claimed that Motorola and America On-line misappropriated its proprietary rights to basketball scores while governments sell the rights to the potentially *Personal Information* they collect. The World Intellectual Property Organisation debates protecting databases and expanding copyright protection for digital works (CFP, 1997). The debate over who owns data has therefore often overshadowed the debate about what makes data sensitive. Clarke (1999) tries to solve this problem by breaking down privacy into 4 dimensions:

- 1) Privacy of the person (about one's body).
- 2) Private behaviour (e.g sexual preferences and habits, political activities and religious practices).
- 3) Private communications (without routine monitoring).
- 4) Private information (data about the individual that they should have control over and restrict access to).

He proposes that it is useful to use the term *information privacy* to refer to a combination of communications privacy and data privacy. The major risk to privacy is suggested to be through *dataveillance* where an individual's actions or communications are systematically investigated. However, what *Personal Information* means is again not defined with any degree of detail. The importance of securing sensitive data has been clearly stated. Recent research has shown that protecting *Personal Information* privacy should increase Internet usage amongst 78% of United States users who already use it and 61% of those who currently do not use it (Harris & Westin, 1998). However, I conclude that the relationship between data, information and privacy invasion has not yet been clearly identified. These issues have probably not been addressed because, again, the driving force behind most research into privacy and information is the concept of *Personal Information*. This author argues that privacy invasion is more complex than merely individually identifiable data.

Internet users were found to be more likely to provide data if they are not identifiable (Cranor, et al., 1999). However, I would argue that there is a wealth of data collected today which many do not

consider as invasive even though it does identify individuals. Loyalty cards can identify how many tins of beans a shopper has bought so as, for instance, to send them money-off tokens for beans. Many people consider this an acceptable trade-off of privacy since the shopper opts into the scheme by obtaining the card and the benefits are considered higher than potential privacy risks. However, if shoppers were automatically put into these schemes (every time a credit card is given for food) this might change their perception of control of the situation thus affecting their acceptance of the potential privacy risks. However, the interaction of *other* variables may seriously effect the user's judgement with reference to privacy invasion. If all the people who bought more than 5 tins of baked beans a week were sent marketing details under the label of 'bean-freaks' would it be the lack of control that people found invasive or the way they were being perceived? This emphasises the different levels at which data can be interpreted. Some types of data are more sensitive than others. Data about a child is far more sensitive than the same data about an adult (Cranor et al., 1999). The type of data that is perceived as highly sensitive information may also be initially counter-intuitive. Cranor et al. (1999) identified that similar types of data can be perceived as having different sensitivity levels. For example, with contact data a phone number was perceived as far more sensitive information than an email or postal address.

Grounded Theory model building

This section partially supports the model factors:

Information Sensitivity: Judgement (Sub-section 8.3.2.1)

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

2.3.2 Who receives the information?

The complexities of privacy issues are further complicated by Bellotti's (1996) suggestion that privacy can be invaded without the user being aware of it. This brings to the forefront the additional question of whether it is what is known about a person that is invasive, or who knows it. This is probably why, the person receiving the data can be a deciding factor in whether someone will provide it or not (Cranor et al., 1999). Many privacy invaders, however, do not see themselves in this way because of the valid reasons behind the invasion and the use to which the information is put (Kling, 1996). They may not consider themselves as invading someone's privacy because of their relationship with the person (e.g. parent). Le Poire et al. (1992) identified a relationship between the type of invasion, the status of the privacy manipulator and strategies that subordinates take to restore their privacy. However, this research does not define the extent of these relationships and the degree of other factors affecting these results (e.g. participants' degree of organisational trust).

Most of the literature on privacy has not clearly identified the role of the person receiving the information. Bellotti (1996) attempts to address this issue by relating privacy invasions to an infringement of user perceived acceptable receivers for their data. However, there is no discussion of how this interacts with the type of data being relayed or the ultimate usage made of the data. It is

interesting, though, that Bellotti & Sellen’s (1993) research at EuroPARC found that privacy was not a major issue here because benefits were traded-off against potential concerns. Users’ reduced privacy fears were identified as due to the general environment of trust and the development of acceptable practices relating to the application’s usage. It could be argued that this suggests trust in those receiving the data can transfer to perceptions of its usage and may decrease its sensitivity (see Table 2.3).





	Trust environment	Distrust environment
Usage perceptions		
Information perceptions		

Table 2.3: Trust in those receiving the information and perceptions of its usage

Buxton & Moran (1990) suggests that legitimate use of systems and security devices should be considered. This brings to the forefront issues of *trust*, legitimate use and confidence in the users (Adams et al, 1997; Adams & Sasse, 1999c). Many of these issues are related to communication and control between the organisation and the user. The balance between these two bodies could affect users’ perceptions of trust levels, confidence and legitimate use. Imposing mechanisms that circumvent communication or user control may create perceived feelings of distrust and a lack of confidence in the organisation by the user thus reducing the perceived legitimate usage of such mechanisms. However, although *trust* is an important factor in privacy perceptions, this is rather a limited view of privacy, which could lead to unreasonable usages of sensitive information being accepted by users. It is dangerous to assume that privacy is simply a question of trust. If only users’ trust levels are addressed we could be designing systems which users’ trust but which, unknown to them and the designers, invades their privacy. I propose that the full complexity of privacy and interactions between trust and privacy must be identified before an analysis of privacy perceptions can be understood.

Grounded Theory model building

This section partially supports the model factors:

Information Receiver(IR): Trust (Sub-section 8.3.3.1) this issue interacts with other factors (e.g. organisational norms, trust) to effect information sensitivity levels.

Information Receiver (IR): Relationships (Sub-section 8.3.3.2) can affect acceptability as an information receiver and also the sensitivity of the information.

Users can trade-off increased privacy risks against particular IR factors (see below)

Information Receiver: Trade-off’s – trust (Sub-section 8.3.3.3)

InformationReceiver: Trade-off’s – roles (Sub-section 8.3.3.4)

Information Receiver: Trade-off’s – group membership (Sub-section 8.3.3.5)

Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

2.3.3 How is the information used?

How data that is personally identifiable is used has always been of key importance to people with regard to privacy and this is the main area where privacy is often noted as having been invaded (e.g. organisations discriminating against people about whom they have obtained HIV data). Users' fears about technology are often said to come down to a fear of mounting data about themselves profiling them in a negative way. However, a lack of contextual data can produce just as much of a privacy problem as too much data being stored. Dix (1990) states that *Private Information* can be closely intertwined together with the context it is viewed within. Privacy is suggested as having a hierarchical nature with data's contextual setting (e.g. specific environmental setting, temporal context etc.) strongly linked at a lower level to potential invasions of privacy. Without this contextual setting information some data's privacy content can increase. Dix further argues that most data usage strips it of important contextual elements, which are the causes of many misinterpretations of the data. Therefore, data taken out context can increase misunderstandings when the data is put back into a meaningful information context, such as a with data profiling.

Bellotti & Sellen (1993) note that *Information Usage* and privacy invasion relate to two issues:

- 1) Computer technology may be used in an unethical way.
- 2) User-interface design features may interfere with social behaviour and thus give rise to inadvertent intrusions of privacy (Heath & Luff, 1991).

However, these two dimensions do not explain the dislike, with regard to privacy protection, that users have for the automatic transfer of data about themselves and their patterns of use. Nor does it explain users feeling their privacy has been invaded when data given to one web site results in unsolicited communications from another web site. (Cranor et al., 1999). It must be asked whether these problems could be due to a breakdown in users' perceptions of trust and control within specific social and organisational settings. Ultimately I propose that interactions between these factors, in technology mediated interactions, must be reviewed.

Grounded Theory model building

This section partially supports the model factors:

Information Receiver: Trade-off's – trust (Sub-section 8.3.3.3)

Information Usage (IU): Later IU – context (Sub-section 8.3.4.4)

Context: Organisational culture – trust (Sub-section 8.3.5.7)

2.3.4 Social and Organisational Issues

It could be argued that what matters is the social or economic system in which technology is embedded, not the technical artefact itself. Winner (1985) argues that technology develops with certain social structures in force, and it is these, and not the technology, that invade people's privacy. The construction and effective daily operation of many systems requires the development of centralised,

hierarchical organisational and social structures without which they will collapse (Chandler, 1977). Krull (1995) suggests that it is organisations striving to survive and prosper that have produced a focus on how to be more productive, yet under the hierarchy's control. Again, however, I would emphasise the importance of the users' perception of control, which may greatly differ from the organisational perspective.

This author also argues that whatever an organisation's approach, it must assess how the relationships between organisational control and trust affect users' privacy. Krull (1995) suggests that the appropriate use of authority is direction, not control, since explicit, inflexible rules undermine trust. Trust is undermined by force sending a contradictory message to people that does not allow them to judge trade-offs for themselves or feel part of the proposed solution. I would also suggest that guidelines and boundaries (but not restrictive controls) encourage and nurture trust that allows for privacy to be secured (and visa versa: see Diagram 2.4).

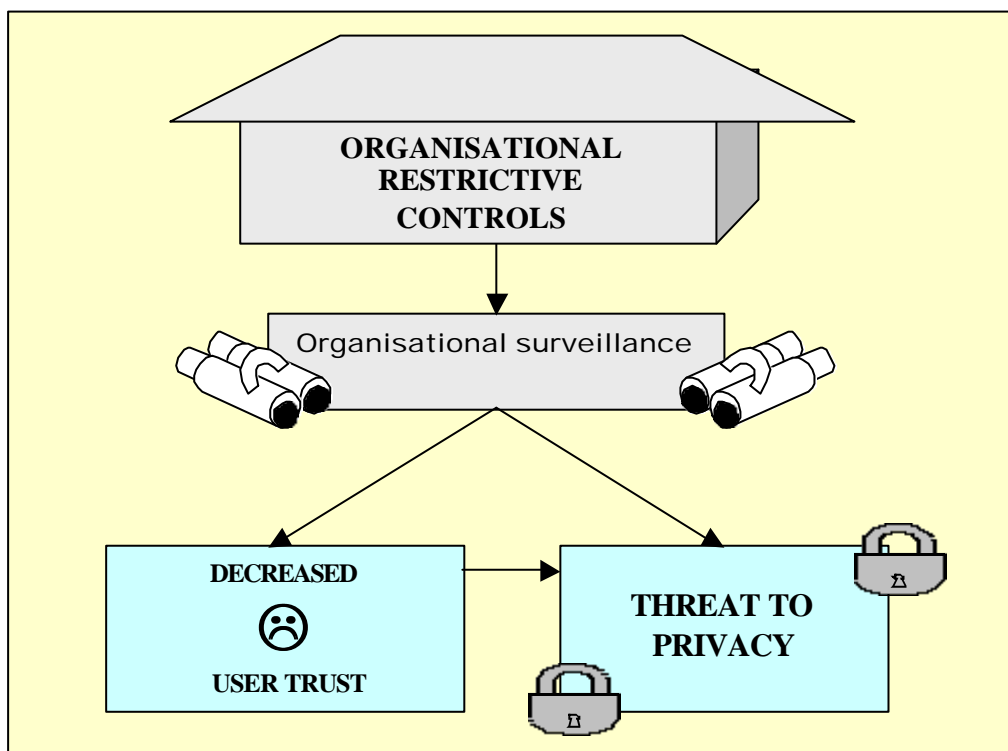


Diagram 2.4: Restrictive organisational controls effect on privacy perceptions

Surveillance technology, on the other hand, has been used to curtail our freedom in a way so as to control and manipulate socially unacceptable behaviour. Jeremy Bentham (1832) argued for control by surveillance, in the preface to his 'Panopticon', whereby every person in a building is watched from a central tower. Although people were not watched all the time, they maintained their standards of behaviour for fear of being watched. Fear would be maintained by examples being made of odd individuals to *'keep the others on their toes'*. Bentham (1832) identified this as an effective strategy because:

“Morals reformed - health preserved - industry invigorated - instruction diffused - public burdens lightened - Economy seated, as it were, upon a rock - the gordian knot of the Poor-Laws not cut, but untied - all by a simple idea in architecture!”.

The ‘Panopticon’s’ modern-day equivalent, closed-circuit television (CCTV), is one of the fastest growing technologies. In the UK, for instance, coverage is such that there will soon be a national CCTV network. Although CCTV provides little or no means of control by those being observed many users accept the potential risks to their privacy (e.g. security staff using CCTV footage for their entertainment or profit) in a trade-off with perceived benefits (e.g. catching criminals). Such trade-off’s are usually made within an environment where the perceived individual risks are low (“I am doing nothing wrong, so I am OK”) and / or the perceived benefits (e.g. personal safety) are high. If such a risk assessment (based on social cues) turns out to be inaccurate, the implications for privacy are far-reaching.

Kling (1996) argues that privacy debates and controversies will only increase with time as organisations expand their systems and techniques. It is noted, however, that continuing with a retrospective response to increased privacy invasions and decreased organisational accountability will only result in greater undefined social costs. The type of response a company takes to privacy issues relates to differing organisational interests and values. Five main value orientations which could aid in understanding social repercussions are identified:

- 1) *Private Enterprise Model*: Primary consideration being profitability of a system above other social values.
- 2) *Status Model*: Primary consideration being power and efficiency of state institutions above other social values.
- 3) *Libertarian Model*: Primary consideration being the civil liberties of individuals above profitability and welfare of the state.
- 4) *Neo-Populist Model*: Primary consideration being that practices should be responsive to and understood by ordinary citizens.
- 5) *Systems Model*: Primary consideration being that financial systems should be technically organised, efficient, reliable and aesthetically pleasing.

It has been argued that systems supporting any of these value models are in the public interest (Kling, 1996). In recent years the debate over direct marketing has centred on the public interest of this activity with its potential to reduce junk mail. Hatch (1996), however, argues that direct marketing firms gather more personally sensitive data than is required and that they should regulate themselves to a higher degree before they are regulated by legislation. He argues for self-regulation producing opt-out and fair information practices. Privacy advocates also argue for self-regulation, which from an organisational perspective usually means opt-in or opt-out information policies (see Table 2.4).

		Market Driven	Regulatory
USERS	Opt - Out ⁴	Business or industry	Consumers
	Opt - In ⁵	Consumers or regulators	Consumers or privacy advocates
	NO CONTROL	Business	Business

Table 2.4: Policy driven divides

These approaches, however, rarely provide clear practical organisational policies or guidelines regarding privacy, partly because there is no clear research to guide them. This is probably why most organisations are not compelled to initiate policies without clear benefits identified behind them.

Grounded Theory model building	
This section partially supports the model factors:	
<i>Information Receiver: Relationships (Sub-section 8.3.3.2)</i> our relationships within a social structure can affect information sensitivity levels and thus related trade-off's made.	
<i>Information Receiver: Trade-off's group membership (Sub-section 8.3.3.5)</i>	
<i>Context: Social groupings – social groups (Sub-section 8.3.5.4)</i>	
<i>Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)</i>	
<i>Context: Organisational culture – trust (Sub-section 8.3.5.7)</i>	

2.4 RESEARCH APPROACHES TO PRIVACY

Over the past 30 years the call for privacy protection has increased along with ubiquitous computing. Sieghart (1982) identified the main proponents in the computers and privacy debate. Namely that if you believe in the good of computers you will not subscribe to the view that they can damage users through privacy invasions. Ten years later the debate between censorship and privacy still continues (Costello, 1991; Boyle, 1997). Many privacy researchers have moved away from this perspective towards an acceptance that privacy problems exist and that there is a need to seek active solutions.

As computer privacy relates to issues of confidentiality, data transmission security and more generally information privacy it is not surprising that computer security specialists have provided a major force behind privacy protection advancements (McGregor, 1992; Spirakis & Tampakas, 1994). In the past, their influence within privacy research has in lead to a focus on the security of data against various risks (Clarke, 1997). However, I would argue that this data-centric approach to privacy protection is based on premises that no longer exist. When identifying computer privacy problems in the Eighties, privacy professionals highlighted the need to regulate data not tasks because it was argued that (Sieghart, 1982):

1. the categories of tasks are comparatively small;
2. the tasks completed are to the mutual benefit of both the user and the *Information Receiver*.

⁴ Opting-out: automatically put the user within the marketing program requiring them to request to opt-out of it.

⁵ Opting-in: a user requests to join a marketing program for disseminating their details or receiving information.

However, I propose that with the increased ubiquity and capabilities of computerisation these arguments no longer stand. This data-centric perspective of privacy has its roots in the technical and military style of many security departments. This narrow perspective, has been claimed, produces security mechanisms which are, in practice, less effective than they are generally assumed to be (Davis & Price, 1987; Hitchings, 1995; Adams, 1999b; Adams 2000).

Although the security perspective still influences many privacy protection approaches (e.g focusing on *Personal Information*) there is an increase in privacy approaches which review privacy as a broader phenomenon. Bellotti (1996) distinguishes between privacy issues that relate to the fields of security and legislation. This distinction appears, in the main, to be reflected by the majority in the privacy debate. However, the 'Computers Freedom and Privacy' conference (CFP:1997) identified two major strands within the privacy discussion⁶:

1. The legislative approach.
2. The technical approach.

2.4.1 Legislative and policy approach

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 the 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). In my view this produces an influx of recommendations by privacy experts on what would increase users' trust without any input from the users themselves. This approach is based on over-simplified assumptions about the data subject (user) and the cause of privacy invasion. It is assumed that privacy invasion is caused merely by a lack of secrecy from those that have someone's *Personal Information* and by what he or she is using it for. I would argue that these assumptions should be reviewed further, especially with reference to users', rather than merely experts', opinions.

Traditional political science approaches to privacy protection take a procedural, due process approach rather than a substantive one (Raab & Bennet, 1998). The individual (whose privacy requires protecting) is defined as the *data-subject* and the organisation using the data as the *data user*. However, it has been argued that this is a rather one-dimensional view towards the *data subject* (Raab & Bennet, 1998). This perspective fails to acknowledge that data subjects' perceptions of privacy invasion risks may differ (personal exposures to risk, perceptions or fears of risk). Although privacy invasion risks can be measured approximately, how this phenomenon varies across social groups and sectors is not taken into account. Some individuals may be more vulnerable (e.g. because of socio-economic backgrounds) than others may be. However, I suggest that although *data-subjects*'

⁶ Grouping and terms identified and named by the author.

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.

Most organisations receiving and using *personal data* have taken a reactive rather than pro-active approach to privacy protection (Smith, 1993; Petersen & Kupersanin, 1996). However, it has been argued that the *data user* should know more about the privacy concerns of their customers, clients, students etc. (Raab & Bennet, 1998). This will help develop the trust bond that it is required by individuals in organisations using, what they consider to be, their information. If organisations lag behind privacy problems, most will retain privacy policies that have been outgrown by changes in either society or the organisation's activities. This then increases the probability that the organisational policies will clash with socially expected privacy norms. Slow to react organisations could increase perceptions of organisational secrecy and Big Brother scenarios (Bellotti & Sellen, 1993). In Smith's (1993) study 50% of interviewees experienced emotional dissonance due to value conflicts with the organisation they worked for. However, I would argue that this organisational retrospection could have its roots in the notion, as previously detailed, that they know better than the individual. This author would suggest that organisations must understand that different contexts have different privacy implications and that privacy relies on the individual's trade-offs and acceptance of certain risks.

Political scientists often note that different kinds of data are reviewed in data protection, but not different kinds of persons or the information perceptions of those people. Some argue that all data can be sensitive, depending on the context of use, but data divisions are generally thought to be (Raab & Bennet, 1998):

1. *Inherently sensitive data*: racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, concerning health or sex life.
2. *Relatively innocuous data*: payroll, household management.

However, this does not take into account that data can change its sensitivity depending on who views it and for what purposes. Raab & Bennet (1998) refer to the concept of *personal grouping data* as placing an individual within a group thereby increasing its sensitivity. I would like to take this argument further by suggesting that highly sensitive data may not be only personally identifiable data but also social grouping data. (a house: family group, a street: geographical bound group, a school: social group). Social grouping perceptions should be considered when reviewing important privacy issues.

Finally, political scientists have tended to concentrate their endeavours on *Information Usage* (Reidenberg, 1993; Bennett, 1997). This focus has emphasised the idea that secrecy in *Information Usage* is the root cause of privacy invasion. Open usage disclosure and procedures and official bodies for complaint are suggested as solutions to those invasions. This is the basis of the fair information principles on which many countries have based their information privacy or data protection policies (Bennett, 1997). However, I would argue that, if the assumptions detailed in this Section are inaccurate

this will produce ineffectual policies missing the privacy invasion point. An example of this can be seen in one organisation's valid endeavour to help produce privacy policies that are based on these assumptions. The web site of the organisation in question (run by a popular privacy advocate) takes the users' email address (meant as a means of direct communication) as a form of user ID. The reasons stated behind this *Information Usage* are to allow for an ID that is both unique and yet memorable. However, this assumes that a unique identifier (a name) is on a similar sensitivity level as an identification medium for direct communication (which it may not be, see Cranor et al., 1999). A user being asked to input his or her email address as a form of User ID could⁷ be worried about the distribution of this data and its later usage. Although these fears can probably be allayed by further feedback, it should be asked whether the threat to users' trust in the organisation's procedures and motives are worth risking. This potential privacy problem probably has its roots in the concept of a personal or not *Personal Information* distinction. This author proposes that many organisations assume that a user providing so-called, *Personal Information* for accepted organisational practices (e.g providing a service) accepts that this can be used in any way that fits within these parameters. This again makes the mistake of assuming that data remains at the same degree of sensitivity regardless of changes in its usage.

Ultimately policy-makers need to understand how privacy issues arise in order to develop appropriate and effective privacy policies for computer systems (Agre, 1997). Policy makers must therefore understand the risks and capabilities of the technology. Marc Rotenberg (1992) has argued that enlisting the help of computer professionals can greatly help in the production of good computer privacy policies. He cites various successful examples where members of the 'Computer Professionals for Social Responsibility (CPSR)' and other computer professionals have helped to develop effective privacy policies.

Grounded Theory model building

This section partially supports the model factors:

Information Receiver: Trust (Sub-section 8.3.3.1)

Information Receiver: Trade-off's group membership (Sub-section 8.3.3.5)

Information Usage (IU): Later IU – context (Sub-section 8.3.4.4)

Context: Social groupings – social groups (Sub-section 8.3.5.4)

Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

Context: Organisational culture – trust (Sub-section 8.3.5.7)

2.4.2 Technical approach

The technical approach to privacy protection has, in the past, focused on providing the user with a control of their privacy rather than, as with the political science approach, providing feedback on organisational policies. The importance of encryption (and thus cryptography) has been paramount in

⁷ This potential problem is verified to some extent by this being detailed as a FAQ on their web page.

these endeavours (Needham & Schroeder, 1978; Diffie & Landau, 1998). However, these technical mechanisms are based on the traditional *Personal Information* assumptions i.e. that potentially invasive information only relates to data that identifies the individual. This approach leads to the conclusion that to anonymise data, or the user, would take away its personal identification and thus secure privacy. However, as mentioned in the previous Section, there is a need to protect the privacy of a social group (see Sub-section 2.4.1). Also, different multimedia environments can provide anonymity but still be perceived by the user as invasive (see Sub-section 9.2.1). Ultimately, as Section 2.3 details, what is potentially invasive cannot simply be defined as data that identifies an individual. Conversely, some data that does identify the individual may rarely be considered potentially invasive (supermarket shopping habits). Table 2.5 highlights this problem by showing the different types of data addressed by current technical mechanisms and who they are seeking to protect.

	Limited data (e.g. <i>Personal Information</i>)	Complex data (e.g. multimedia data)
Individual	Cryptography, encryption, PGP	Not fully addressed (To some extent, watermarking and water casting)
Social group	Currently not addressed	Currently not addressed

Table 2.5: Users and data that privacy mechanisms seek to address

The development of technical mechanisms, such as *public key cryptography*, acknowledges the importance of who is receiving the data (Diffie & Landau, 1998). However, I would suggest that identifying the acceptability of the recipient for specific data is not, as is often assumed, a simple matter. A recipient may be acceptable for certain types of information or in certain situations but these are constantly changing. Relying on the user detailing the acceptability of the recipient under different conditions would lead to unreasonable user costs (time, effort etc.) and complex user interfaces. This is probably why some of these systems have been noted as having serious usability problems (Whitten & Tygar, 1999). I would propose that a cause of many of these problems is that in developing privacy mechanisms there is a need to operationalise complex, fluctuating phenomena such as trust. If the system does not operationalise the phenomena they rely on the user making time-consuming trade-off decisions for every situation.

Finally technical mechanisms have sought to address privacy invasion risks associated with data usage (primarily multimedia data). With the aid of watermarking and watercasting the copying and editing of multimedia data can be identified and potentially traced (Brown et al., 1999; Craver et al., 1998). Copied multimedia data, once identified, could be traced back to its origins. However, these mechanisms are not automated, and thus rely on the user trawling through data trying to find if their data is on public display somewhere. Furthermore, there is no mechanism that would inform the person receiving the data that it has been tampered with *against* the users' wishes. I would argue that receiving data without adequate feedback of users' acceptability levels for its usage, restricts the development of social norms for acceptable practices in information usage.

Grounded Theory model building

This section partially supports the model factors:

Context: Technology – interface issues (Sub-section 8.3.5.2)

Context: Social groupings – social groups (Sub-section 8.3.5.4) with relation to social grouping privacy

2.4.3 Semantic cueing approach

A more recent approach to privacy protection has started to peruse, in a vague way, users' requirements for privacy needs. This movement has sought to increase user perception of privacy protection through providing both *feedback* and *control*, encouraging trust in systems. Schemes that present the user with opting-in or opting-out clauses are supposed to increase user's perception of control of their data whilst often presenting feedback of how the data would be used by the organisation in question (CFP, 1997). It is suggested by this thesis, however, that this apparent control may be an illusion. Users often skim read complex privacy policies and organisations omit potentially damning specifics of data usage. Also, although opting-in gives a far higher degree of control to the user than opting-out (due to user-costs, i.e. time, effort, money), organisations have tended to adopt the former rather than the latter (Sub-section 2.3.4).

Trust badges or seals are a symbol to users that the web site in question is following specified guidelines in their privacy practices (Benassi, 1999). Often these follow the fair information practice guidelines of a willingness to disclose *Personal Information* dissemination procedures backed by a credible third-party assurance of these practices. The hope is that these badges will encourage users' trust and confidence in these web-sites while also helping the Internet to self-regulate privacy practices. However, I would suggest that users' trust in the badges only extends as far as they trust the organisations that administer them. As many of these organisations did not exist prior to the Internet their reputation is unfortunately not well established. It is also important to note that the privacy policies that subscribing sites ascribe to have been directed by the legal or policy approach to privacy and thus retain many of those limitations (see Sub-section 2.4.1.).

In recent years the worldwide web consortium (W3C)'s Platform for Privacy Preferences Project (P3P) has tried to bridge the gap between the legislative or policy, technical and semantic cueing approaches (Reagle & Cranor, 1999). The aim of this project is to provide users with feedback about web-site practices whilst having the control to specify their relationships, and thus data disclosure, with specific sites. To reduce user overheads, it is suggested that many decisions, at the users' discretion, could be delegated to computer agents (Ackerman, & Cranor, 1999). It is hoped that this project will increase users' confidence in on-line transactions. However, all of these semantic cueing mechanisms (e.g trust badges, opting-in vs. opting-out, P3P) rely on accurate appraisals of users' perceptions of privacy. If the related policies are based on inaccurate representations of users' privacy perceptions they will not address users' current and future fears.

Grounded Theory model building

This section partially supports the model factors:

Information Receiver: Trade-off's – trust (Sub-section 8.3.3.3)

Information Receiver: Trade-off's – roles (Sub-section 8.3.3.4) P3P could allow the user to denote who has an appropriate role as an information receiver.

Context: Technology – interface issues (Sub-section 8.3.5.2)

2.4.4 User perceptions

A major proposition of this thesis is that privacy relies on how we perceive it. How private or safe we are may not necessarily be as important as whether we perceive ourselves to be safe and private. In 1982 Dr. John Dawson presented a case for the British Medical Association and data protection from the perspective of the patients. He argued that only the patient could determine the confidentiality of specified data, as only they understood the full context of its interpretation as information. However, patients' perceptions of their information are rarely obtained while previous problems in data protection (e.g. organisations discriminating against employees who they know have taken an HIV test) have helped to define all medical data as potentially highly sensitive.

Some argue that the slow movement by organisations to ensure privacy is not due to an unwillingness to be the first to take action but to a lack of clearly defined boundaries and action that needs to be taken (Smith, 1993). This author proposes that without clearly defined negative outcomes from not ensuring users' privacy there is little incentive for organisations to protect it. It should also be noted that, without detailed accounts of users' privacy boundaries and levels of information importance there is little guidance for organisations when determining company or system privacy policies. Ultimately I would suggest that until a validated account of users' perceptions is identified and detailed, with some accuracy, there will be little movement by organisations in ensuring privacy (see Diagram 2.5).

National opinion polls (off-line and on-line questionnaires) have sought to capture users' perceptions to help direct privacy protection advancements. However, the results from these surveys have done little more than identify the importance of computer privacy for users' (Harris & Westin, 1998; Cranor et al., 1999) and substantiate privacy advocates' perceptions of data usage. It is argued by this thesis that incomplete findings may be the result of an approach which is not adequate as an exploratory tool for a complex and previously under-researched phenomenon such as computer privacy. Recent questionnaires have sought to delve more into the specifics of users' information perceptions (Cranor et al. 1999). However, with the fast changing nature of computer technology potential privacy problems are often not recognised until they occur. Within the field of multimedia communications a need to keep ahead of potential privacy problems has led to an increase in privacy policies based on anecdotal findings (Bellotti & Sellen, 1993; Mackay, 1995). Although this approach may uncover some important issues, without a holistic appraisal it may only highlight idiosyncratic problems for specific situations and organisational cultures (Dourish, 1993).

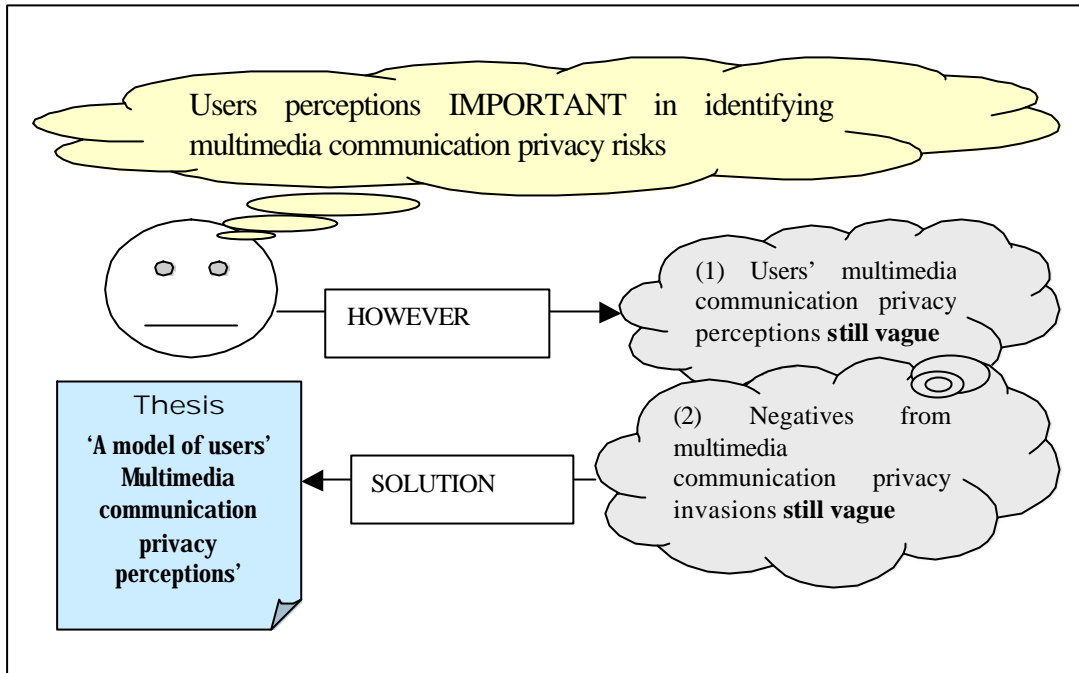


Diagram 2.5: Users' perceptions in multimedia communications

2.5 CHAPTER SUMMARY

Looking at previous social science literature we can see that *social, cultural, physical* and *contextual cues* guide users' situation perceptions, their appropriate behaviours and acceptable privacy loss trade-offs. (see Section 2.1). Privacy specific research, though, has centred on *Personal Information* relating to expert opinions of invasive identifiable data (see Section 2.2). Causes of privacy invasion, however, are more complex than malicious intent, individual or cultural differences (see Section 2.3). Ultimately previous research highlights that user controls and social norms are important in users' perceptions of privacy levels & emotive responses to privacy invasion (see Section 2.4). Social relationships, trust, organisational control and information perceptions can also increase the limit of what is acceptable in data interception and usage (see Sections 2.1 and 2.4). Ultimately privacy research has moved away from its justification to a data-centric attitude that is slowly being overshadowed by a broader approach (see Section 2.4).

A Grounded Theory summary of the research reviewed in this chapter is presented in Table 2.6. This representation shows how previous research from this chapter contributes to the privacy model being developed, where the gaps are currently in the model and how the following chapter will expand on the model.

Model Factors	Chapter 2 Privacy model contributions	Gaps in the model	Chapter 3 Model development
USER FACTORS		This research does not review the user factors of privacy with relation to their interaction with technology.	Privacy research into user perceptions within multimedia communications environments will be reviewed.
<i>Mental models</i>	Section 2.1 & Sub-section 2.1.1		
<i>User Distinction</i>	Section 2.3		
INFORMATION SENSITIVITY (IS)		This research does not review the specific relevance of <i>Personal Information</i> in multimedia communications and subsequent trade-offs.	Research into technology specific information perceptions and resultant trade-off's made are reviewed in the next chapter.
<i>IS Judgements</i>	Section 2.3 & Sub-sections 2.2.2, 2.3.1		
<i>Public / private situation</i>	Sections 2.1 & 2.3		
<i>Primary / secondary information</i>	Sub-sections 2.2.1, 2.2.2, 2.2.4, 2.3.1		
INFORMATION RECEIVER (IR)		This research does not identify, the exact relationship between <i>task, situation, social groupings, control, feedback and perceived privacy</i> specifically within multimedia communications.	The following chapter reviews research on the information receiver factors already highlighted here within multi-media communication environments.
<i>Trust</i>	Sub-sections 2.3.2, 2.4.1		
<i>Relationships</i>	Sub-sections 2.3.2, 2.3.4		
<i>Trade-off's – trust</i>	Sub-sections 2.3.2, 2.3.3, 2.4.3		
<i>Trade-off's – roles</i>	Sub-sections 2.3.2, 2.4.3		
<i>Trade-off's – group membership</i>	Sub-sections 2.2.3, 2.3.2, 2.3.4, 2.4.1		
INFORMATION USAGE (IU)		The research in this chapter does not review information usage issues of repeated viewing, editing, risk / benefit trade-off's.	Chapter 3 reviews research within multimedia communications, of various information usage privacy issues and <i>trade-off's</i> made
<i>Current IU – task</i>	Sub-section 2.1.1, 2.3		
<i>Later IU – recording awareness</i>	Sub-section 2.1.1		
<i>Later IU – Context</i>	Sub-sections 2.1, 2.1.2, 2.3, 2.3.3, 2.4.1		
CONTEXT		The previous research reviewed in this chapter does not relate contextual issues specifically to technology or identify the effect of inaccurate or non-existent virtual environment <i>cues</i> on privacy perceptions within multimedia communications.	The following chapter will review research that relates contextual issues to multimedia communication environments as well as privacy issues specific to these environments and contextual factors.
<i>Technology – interface issues</i>	Sub-sections 2.1.1, 2.4.2, 2.4.3		
<i>Technology – presence</i>	Sub-section 2.1.1		
<i>Social groupings – social groups</i>	Section 2.1, 2.3 & Sub-sections 2.2.4, 2.3.4 2.4.1, 2.4.2		
<i>Social groupings –outsiders</i>	Section 2.1		
<i>Organisational culture –norms</i>	Section 2.3 Sub-sections 2.3.2, 2.3.4, 2.4.1		
<i>Organisational culture – trust</i>	Sub-sections 2.3.3, 2.3.4, 2.4.1		
<i>National & international cultural norms</i>	Sub-section 2.1		

Table 2.6: Grounded Theory summary of interdisciplinary research, model contributions and gaps

Chapter 3: Multimedia communications and privacy

Multimedia communications has its roots in the 1950's with the picture-phone (Video-phone), the first two-way audiovisual communication device. In 1956 a picture-phone test system first transmitted audio and an image once every two seconds (AT&T, 1999). In 1964 an experimental system was developed but user trials revealed that people did not like using the system. Many usability problems were dealt with and in 1970 a commercial picture-phone service debuted, which was predicted would sell a million sets by 1980. This optimistic prediction was not realised and the project lost millions of dollars. Noll (1992) reviewed the failure of the picture-phone and argued that the widespread use of videophones was unlikely to *ever* succeed. He added that the cause of the picture-phone's, and potential successor's, failure was due to the fact that "*customers had no applications for it*" (p.315). Noll also argued that the failures of the picture-phone are the root flaws of videoconferencing. However this over-riding negative approach to videoconferencing does not take into account the impact of surroundings, context of use and privacy on the picture-phones downfall (see Section 3.2).

Kraut & Fish (1997) divide up potential videotelephony usage into those of business and residential. They argue that videotelephony should be viewed as an enhanced version of conventional telephony and as such will be successful for similar tasks and within similar surroundings. However, since there was no data to base residential videotelephony predictions on, they assumed usage would not differ from traditional audio telephony patterns. This author argues that this is an invalid assumption to make as the degree of social cues, and thus social implications, of each media are vastly different. Kraut & Fish (1997) concede that it is likely that there are some privacy implications with this technology particularly in residential surroundings. The Personal Technologies research (1993) confirmed this when almost a quarter of residential customers who were questioned, stated that a videophone within the home was an invasion of privacy. Kraut & Fish (1997) argue that to correct privacy problems, users must, as a minimum, have control over whether video images are sent or not. However, I propose that within the residential setting even providing this control contains inferences, which could invade privacy. Providing a video transmission facility in the technology allows for social cues to be released even when the technology is turned *off* (e.g. "what is it that they don't want me to see?") Value judgements, about the users, are also likely to be made by turning the technology off (e.g. "are they shy, unconventional, non-communicative?"). Finally, as Kraut & Fish make a clear distinction between business (including educational) and residential multimedia communication needs and user perceptions only the former will be reviewed within this thesis (see Section 1.2).

3.1 MULTIMEDIA COMMUNICATIONS TECHNOLOGY

Multimedia communications can vary between interaction parties so that they are synchronous or asynchronous, local or remote and from one-to-one, one-to-many and many-to-many. Although there are many systems and applications which could be termed multimedia communications three distinct

forms are reviewed by this thesis; Videoconferencing, Internet Protocol (IP) multicast and Virtual Reality.

3.1.1 Videoconferencing

The history of videoconferencing has developed chronologically with advances in the technology. Finn (1997) reviews the stages of multimedia communication starting with the close-caption TV (CCTV) with dedicated lines transmitting (real time) video directly to participants. However, video conferencing really began with the transmission of group images from one room to another via a common monitor (Isaacs & Tang, 1997).

Multimedia communications came into their own with the advent of desktop videoconferencing. Users sit in front of their computer and communicate in real time via a microphone, camera and – often – a digital workspace (see photograph 3.1). This configuration is often referred to as a *picture-in-a-picture* (PIP) setup.

Photograph 3.1: Desktop videoconferencing

The communication can take place on a point-to point basis or can involve many individuals and sites. Finn (1997) highlights that, with the advent of desktop conferencing, there has been a change of perspective in architecture design towards more support for specialised tasks. This thesis author proposes that this focus shift may have increased a concentration on privacy issues specifically in multimedia environments (e.g portholes, media spaces).

Over the last 10 years there has been an introduction of the concept of *media spaces*. *Media spaces* allow distributed users access to one another via video and audio links (Bly et al., 1993). Networking technology provides collaborative work groups with a flexible, dynamic shared *media space* environment. Like videoconferencing systems, media spaces usually support explicit and intentional

interactions as well as shared artefacts. However, it has been argued that *media spaces* also support informal interactions and awareness (Smith & Hudson, 1995). These informal behaviours are typically found in work groups that share a physical space. Informal communications (colleague presence, activity and availability awareness, and unplanned interactions) have been identified as critical to effective group work (Bly et al., 1993).

Finally *awareness technologies* allow distributed workers to be aware of their co-workers and of their potential for collaboration (Tang & Rua 1994; Narine, 1997; Girgensohn et al., 1999). Awareness technologies invariably use video images as the main data source for awareness. However, some research has argued for the vital importance of audio awareness tools (Smith & Hudson, 1995). *Portholes* (see Diagram 3.1) is a visual tool which provides an integrated view of collaborative members. Porthole images are often presented in a matrix (tiled) format with still images automatically updated at selected intervals (e.g. every 5 minutes) rather than continual data streams .

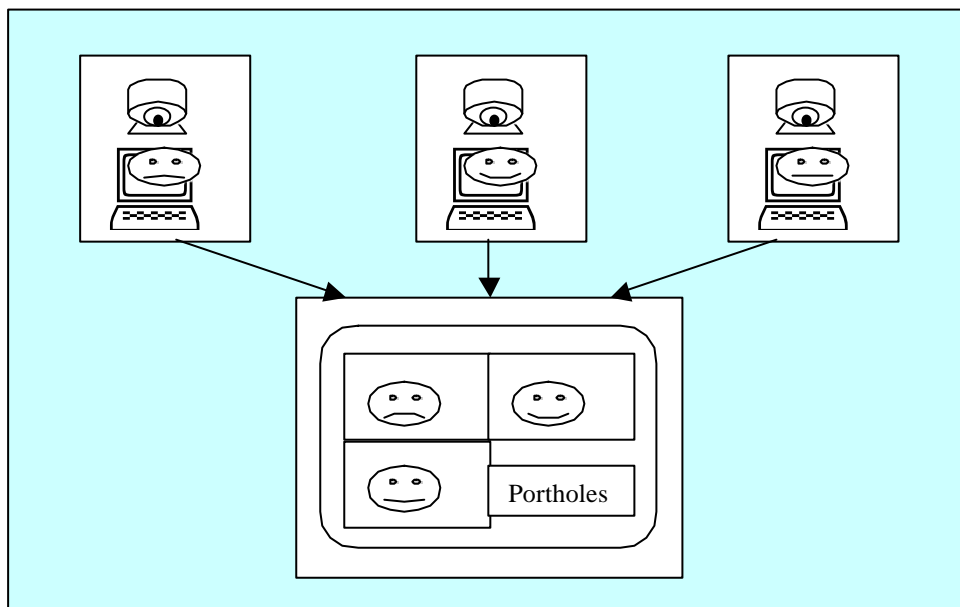


Diagram 3.1: Portholes (matrix style) image layout

3.1.2 Internet and Multicast

Within a shared network such as the Internet data is routed to its destination via a process called *switching*. IP networks require end-systems and routers through which the data is sent. Initially, circuit switching was used for exchanging data over a *physical* path. With the endeavour to more effectively transmit multiple data streams over a network came the concept of *packet switching*. With this process data streams are sent in separate sections, with no set route between two end-systems, and re-assembled once they reach their destination. Packet switching, whilst effectively using the network can make it unpredictable as shared bandwidths and the network traffic varies beyond its capabilities. With a network overload packets may be discarded and the end-systems left to deal with the loss of

data. Packet loss can have a dramatic effect on communications as images and audio become less discernable (see Diagram 3.2)

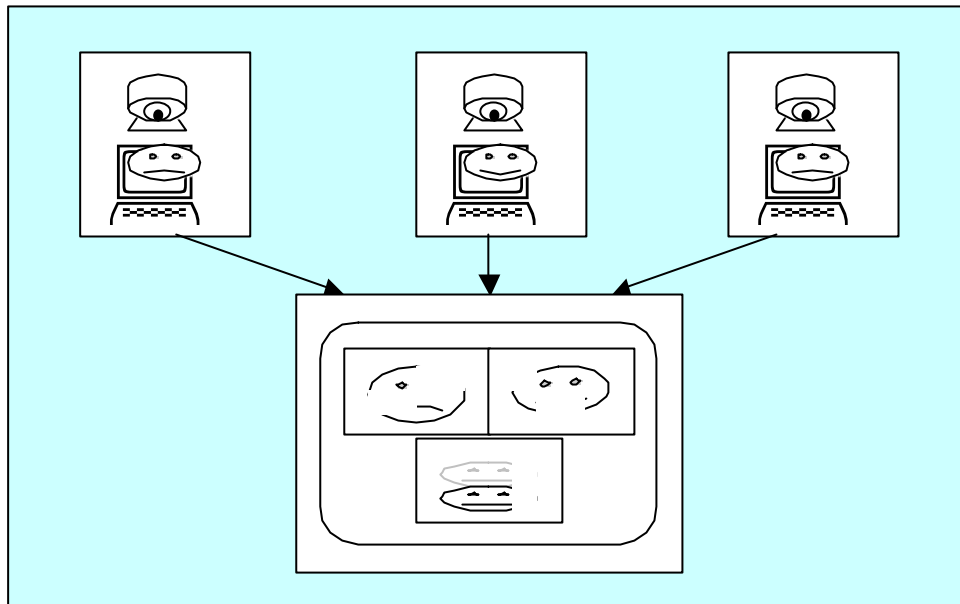


Diagram 3.2: The effect of packet loss on video transmission.⁸

Internet-based videoconferencing has been regularly used since the early 1990's . However, the first major enhancement to Internet videoconferencing has been the advent of multicast. A *Unicast* connection transmits data on a point-to-point basis whilst a *Multicast* connection allows for data to be transmitted to multiple recipients. During *Multicast* the network replicates (at the routers) the packets transmitted. The replicated packets can be sent to as many recipients as have requested the data and are members of the *Multicast* group. Crowcroft (1997) compares *Multicast* to radio and TV broadcasts and highlights that although they are comparable *Multicast* is fundamentally superior to broadcasting. Broadcasts has *one to all* proprieties, whilst multicast transmits from *one to however many is in the group*. Since *Multicast* has greater control over restricted transmissions it also has privacy advantages over broadcasting.

In *multicast* conferencing, audio and video are sent in different streams. These can then be played out either:

1. as they arrive – asynchronous - the audio before the video or ;
2. together – synchronous – audio and video together. This can put a fairly high load on the workstation processor

Desktop conferencing facilities on computer workstations, can use a combination of multicast conferencing tools e.g. *rat* for audio, *vic* for video and *wb* a shared whiteboard (Kirstein et al., 1995).

3.1.3 Virtual Reality

Virtual reality is a computer-based application which allows human-computer and human-human interactivity through a sensory environment called the *virtual world* which is *dynamically* controlled by the user's actions. Virtual environments rely heavily on the notion of immersion both physically and cognitively. Keyboard and monitor input devices allow a user to be partially immersed whilst head mounted displays produce total-immersion in the environment (see photograph 3.2). A user is cognitively immersed in the environment when they feel immersed in the action (Tromp, 1995; Fluckiger, 1995).

Initially virtual environments were used for entertainment and training purposes. Virtual simulations of complex real world systems have been used as learning environments for various conditions (Smets et al., 1995). However, the objectives of virtual reality have digressed into three main themes (Fluckiger, 1995):

- 1) The user's exploration of the virtual world.
- 2) The user's actions on the real world through virtual replications (simulations).
- 3) The user's interaction with other users' participating in the virtual world.

Collaborative virtual environments provide remotely located users with the ability to collaborate via real interactions in a shared artificial environment (Brna & Aspin, 1997). The advantages of virtual reality for collaborative learning is frequently argued by constructivists⁹ to relate to the importance of authentic context (Vygotsky, 1978). Virtual reality (VR) communication environments have been argued to provide a natural, intuitive environment for communication whilst releasing some of the social taboos from social interactions (Kaur, 1997). However, I would add that as virtual worlds increase in their appearance as accurate replications of reality there is an increased likelihood that users will make inaccurate assumptions about the world's capabilities and limitations (see Chapter 2). For example, a realistic VR office environment could produce user assumptions that the environments walls and doors retain real world characteristics, thus implicitly making conversations within a VR room appear private when it is actually public. To date, this has not been empirically tested and should be reviewed to identify any privacy implications.

⁸ This is not real representation of the affect of packet loss but a stylised representation.

⁹ Constructivism is a predominant psychological process theory in collaborative learning virtual environments. They highlight the importance of learning environment actions, real interactions and translating abstract concepts into those that are concrete. For further information see Vygotsky (1978).

Photograph 3.2: Total immersion virtual reality

Virtual actors aid the user in two ways to interact naturally with others in the virtual reality environment. Firstly, virtual actors can represent the user within the environment as an *avatar* (Granieri & Badler, 1995). A user relates and collaborates with other users via their *avatars*. Secondly a virtual actor can represent a software agent with the actor's behaviour defined by that agent.

Grounded Theory model building

This section partially supports the model factors:

Context: Technology – environments (Sub-section 8.3.5.1) this is detailed for video conferencing, Internet, multicast and virtual reality environments.

3.2 BACKGROUND TO MULTIMEDIA COMMUNICATIONS AND PRIVACY

Looking back over the history of multimedia communications, the importance of users' privacy fears can be observed in the downfall of the picture-phone. Initially, users found the system too bulky, the controls were too unfriendly and the picture was too small. However, despite these problems being corrected, the system was still commercially unsuccessful (Noll, 1992). Some still argue that the picture-phone will make a comeback as the technical problems which caused its downfall have been, mostly resolved (Carroll, 1999). However, it has been argued that technical problems were not the source of its downfall (Holtzblatt, 1999). I propose that issues of users' privacy were the cause of the system's failure.

To highlight the privacy implications of the picture-phone this thesis compares its historical development to that of other multimedia (one-way) communication devices. Radio and television have their roots in the theatre (a semi-interactive public activity) and literature. With the introduction of radio this one-way communication device took theatre and literature into peoples homes as a non-interactive semi-private activity. People could now enjoy plays, news and current affairs items from the comfort of their home. With the advent of television people had one-way multimedia communication that was still private. However, unlike the picture-phone, technological limitations (system bulky, the controls unfriendly and the picture small) did not stop people buying television sets. The technology advanced as the market and demand increased.

The picture-phone has its roots in the point-to-point communication of the telegraph and the first public telephones. This public communication situation and technological limitations (bulky, poor controls and audio quality) meant that the medium focused on simple conversations and emergencies that could be better communicated with synchronous dialogue. When the phone moved into the home its usage increased. However, with the technology relying on an operator and the apparatus usually situated in the hallway the privacy of communications was limited and conversations often semi-formal. With the removal of the operator the phone became a private medium which moved into every room in the house with conversations often becoming intimate and personal (Holtzblatt, 1999). The picture-phone moves the phone into a semi-public scenario (back out in the high-street) with users transmitting images which have privacy disadvantages and limited advantages over the current telephone technology. The argument that picture-phones can allow the user to turn off the image misses the hidden meanings that can be communicated in that action ("*why have they turned their image off, what are they doing?*"). Ultimately I would like to infer from this technology an important issue in assessing privacy levels: the location of the technology and thus the accessibility of the information transmitted via situation bystanders (see Table 3.1).

		Location	
		High Street (public)	Home (private)
Accessibility	Public	Phone – publicly open	Phone tapping
	Semi-Private and Public	Phone Box or mobile phone	Picture-Phone
	Private	no technology	Current home phone

Table 3.1: Technology across locations and privacy levels

Modern advancements of the picture-phone in the form of videoconferencing have taken the system interaction back into a semi-public situation within the work place (Holtzblatt, 1999). It is important to review the public or private situation divide with multimedia advancements such as tele-working and interactive television. Privacy debates are already taking place about the monitoring (surveillance) of interactive television usage in the home (Barco, 1999).

Grounded Theory model building

This section partially supports the model factors:

User factor: system interaction (Sub-section 8.3.1.3)

Information Sensitivity: Public / private situation (Sub-section 8.3.2.2)

3.2.1 Culture of multimedia communications

There is a culture specific to multimedia communications, which allows for the free exchange of information reliant, to some degree, on trust. Terms such as *telepresence* and *awareness technologies* are often used to highlight the benefits of information exchange rather than potential risks¹⁰. However, this trust scenario is dependent upon small, within community, settings. Some technologies (e.g. media spaces) that are specific to organisational workgroups have been found to reflect different cultural perspectives even within the same organisation (Dourish, 1993).

The degree of anonymity within some multimedia environments is a major privacy issue within multimedia interactions (Carnevale & Probst, 1997). Being treated as an identifiable individual, rather than an abstract entity, leads to a loss of anonymity that, on some occasions, can produce a loss of self-respect (Schoeman, 1992; Laurel, 1993; Reeves & Nass, 1996). If, in the real world, someone buying their fifth tin of baked beans that week was congratulated at the till and asked to join the ‘bean-freaks club’ - would it be the situation, the label given, the lack of anonymity (i.e freedom of individuality) while shopping or all of these that was invasive? It is interesting to note the advantages that can be

¹⁰ Davies (1997) notes that positive social persuasion has been successfully used within Britain to increase security camera usage. However, this acceptable trade-off relies on user assumptions.

obtained from anonymous computer-mediated interactions. Connolly, et al. (1990) found that anonymous subjects produced significantly more original ideas in brainstorming sessions than those who were identifiable. Within different multimedia communication domains the user can perceive different levels of anonymity. A virtual reality system can provide an increased sense of anonymity compared to a videoconferencing system. The anonymity of many multimedia environments provides users with control over their interactions with less social risk lowering interaction inhibitions (Kaur, 1997). This allows the user the privacy for freedom of expression free from the limits of social norms. Ultimately a private space used for free expression, not restricted by social norms, contains highly charged emotional items which are therefore more sensitive (intimate and private) than a private space in which our behaviours are governed by social norms. (Schoeman, 1992). Although, I would like to add that, as previously mentioned (see Sub-section 2.2.4), this freedom to express oneself relies on the users' perceptions of privacy levels being accurate.

A paradox occurs, however, with a freedom from social barriers in that this can also encourage anti-social behaviour (irresponsible, rude, obnoxious, sexual harassment) which can, in turn, cause invasions of privacy. The cause of these unreasonable behaviours is due to a belief that actions in the virtual world are not accountable for in the real world whilst anonymity aids the impersonal treatment of people (Curtis, 1997). It has also been argued that with computer communication environments' a lack of anonymity (senders and receivers identified) has reduced the incidence of harassment and misrepresentation in networks (Carnevale & Probst, 1997). Nonetheless, as previously pointed out by this thesis (see Sub-section 2.4.4), the importance of users' perceptions when reviewing these issues must not be underestimated. Conversely, relying merely on trust to retain privacy within a medium and community can be dangerous. Privacy invasion may occur unintentionally and be reacted to negatively, even by technology advocates who may be a little less free with their data next time. This author would argue that communication between the *user* and the *Information Receiver*, with regard to privacy, is required so that social norms of acceptable behaviour can be constructed. Virtual worlds can be isolating environments requiring new forms of socially communicated norms.

Grounded Theory model building

This section partially supports the model factors:

Information Receiver: Trust (Sub-section 8.3.3.1)

Information Receiver: Trade-off's – trust (Sub-section 8.3.3.3)

Context: Technology – presence (Sub-section 8.3.5.3) relates to anonymity

Context: Social groupings – social groups (Sub-section 8.3.5.2) vary within organisations

Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

3.2.2 Technology distorting the data

People need social cues to develop mental models about the type of situation (e.g. public, private) in which they find themselves and the type of behaviour with which they should respond (Goffman, 1969). We also use social cues to assess who we are interacting with and how we think others perceive us (see Section 2.1). Multimedia environments vary in the level of contextual cues provided that enable users to appropriately frame their interactive behaviour. (Harrison & Dourish, 1996). Privacy problems, therefore, often occur when people who *are observed* cannot *see how they are being viewed*, by whom, and for what purpose (Bellotti, 1997; Lee et al., 1997). This thesis proposes, that users are likely to make assumptions about who is receiving the data and how accurate a picture of them they are observing, when this assumption is not supported by the technology.

Interpersonal distance has been found to dictate the intensity of a response: faces in a close-up are scrutinised more often than those in the background. Reeves & Nass (1996) argue that, because the size of a face is more than just a representation of an individual, it can influence psychological judgements of a person and thus become an invasive piece of information. Similarly, I would propose that image quality and camera angles may result in a perception of the user that they regard as inaccurate (see Diagram 3.3). A lack of feedback to those releasing the data about how it looks when received may produce inaccurate assumptions about the interaction. However, there is still little research about these perceptions in multimedia environments and still less about how these perceptions affect privacy.

Technology can be used, intentionally or unintentionally, to distort assumptions made by those using it. A system allowing someone to freeze their video streams (e.g. so that they appear to be avidly viewing the screen but instead have actually gone to make themselves a cup of tea) could produce an inaccurate appraisal of their attention within the interaction. This scenario could also produce a mismatch between who is actually watching the images and the assumed (from the frozen image) person receiving the data. Similarly inaccurate assumptions could also occur because multimedia communication environments often lack social, physical and context cues required for users to accurately judge the situation and adapt their behaviour accordingly.

Environments that do not provide feedback about how or why another person is obtaining data can increase privacy invasions through the inaccurate assumptions made. Poor feedback in a videoconferencing environment, where a user's image has been enlarged, produces the misconception that no-one is staring directly at them. In turn the user does not adjust their behaviour accordingly, as they would if someone were staring directly at them in the real world. Conversely, poor feedback about why someone is standing in front of, or following a user (environment movement usability problems) can produce the misconception that they are being followed and stared at when they are not. Behaviour adjustments with restricting data disclosure are based on inaccurate assumptions.

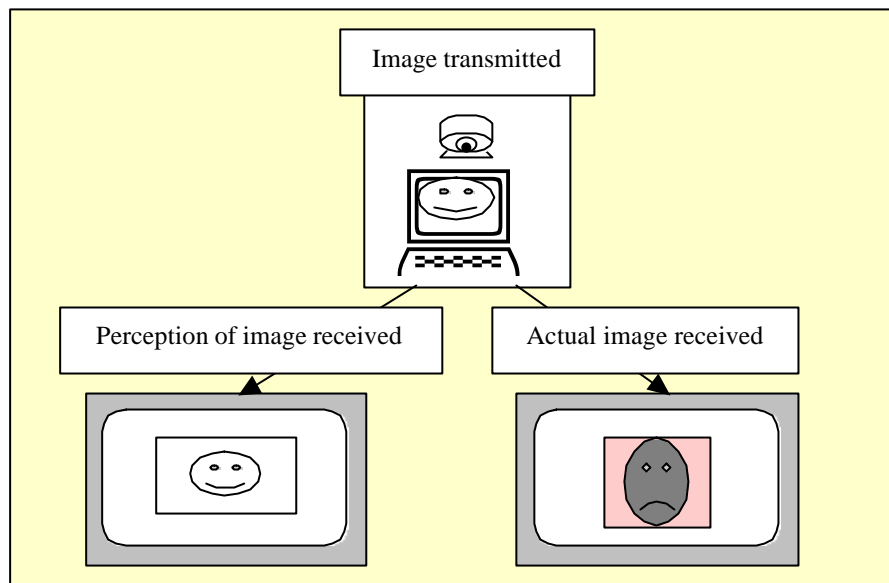


Diagram 3.3: Inaccurate perceptions about image received

The user is not the only one who can feel isolated within multimedia environments due to a lack of feedback. The person receiving the data often does not receive feedback about how their actions or potential actions with the users' data may invade the users' privacy. In the real world standing too close to someone or staring at them for too long would result in disapproving looks, coughs, sighs etc. A lack of the facial and body cues that we take for granted in real world situations can produce an isolating and inhibiting situation for a user.

Some researchers have realised the importance of body cues and gestures within these environments and are seeking to replicate them (Rime & Schiaratura, 1991; Marsh, 1998). Ultimately there is a need for accurate contextualisation of data for all parties within multimedia interactions. The more appropriate social interaction feedback parties receive the easier it will be to develop social norms for acceptable behaviours within these environments. Dourish (1993) argues that if a system is embedded in the organisational culture, social controls will establish a culture of use that will restrict unacceptable activities. I would argue that although social controls are vital (especially in flatter more open organisations) relying on them as the only safeguard for privacy is insufficient. It is important to understand that trust and thus social control evolves with a new technology. To nurture this the technology must not breach users' privacy assumptions especially if those assumptions are based on social cues that are distorted by the technology.

Grounded Theory model building

This section partially supports the model factors:

User factor: system interaction (Sub-section 8.3.1.3) with relation to social cues

Information Sensitivity: Judgement (Sub-section 8.3.2.1)

Information Sensitivity: Public / private situation (Sub-section 8.3.2.2)

Information Usage (IU): Later IU – recording awareness (Sub-section 8.3.4.2)

poor feedback can affect recording awareness

Information Usage (IU): Later IU – context (Sub-section 8.3.4.4) transmitted

information out of context can be misinterpreted.

Context: Technology – environments (Sub-section 8.3.5.1)

Context: Technology – interface issues (Sub-section 8.3.5.2)

Context: Technology – presence (Sub-section 8.3.5.3) and interpersonal distance

3.3 PRIVACY RESEARCH IN MULTIMEDIA COMMUNICATIONS

Moore (1997) points out that a failure to address privacy issues is "*likely to be a source of stress that could negatively impact adoption*" of new technologies (p.307). In a recent poll (Harris & Westin, 1998) the majority of respondents were more concerned with invasion of privacy via online communication than phone or paper-based communication. These findings stress users' need for on-line privacy protection. However, it is interesting to note that a review of email privacy has identified misconceptions about the degree of privacy afforded by the technology (Weisband & Reinig, 1995). These factors together emphasise both the vital requirements for privacy protection mechanisms and explain the lack of protest about poor current protection levels (i.e. 'people think they have more protection than they do')

Multimedia communications originally moved from the traditional videoconferencing paradigm to that of media spaces to encourage casual interactions. To support these casual interactions, it was considered vital to operate in a continuous fashion (typically between whole groups). The constant connection nature of media spaces increases immediate awareness and serves as a catalyst for communications (Hudson & Smith, 1996). However, continuous video data release has led to some users' unwillingness to leave cameras turned on. *Portholes* were suggested to partially solve this problem by periodically transmitting small video snapshots instead of video streams (Dourish & Bly, 1992). Hudson & Smith (1996) suggested it was more a matter of a dual tradeoff between privacy and awareness, and between awareness and disturbance. This thesis literature review (see Section 2.2), however, has identified the apparent importance of privacy controls. Isaacs & Tang (1997) specifically note that although users may not take advantage of privacy controls they will not even experiment with a system without the possibility of blocking access.

“It would be a mistake to try to convince someone that they don’t need access control because most people don’t use it. They “use” it to feel comfortable that the system will let them control their privacy.” (p.193-194)

In other words privacy controls act as a kind of safety net that, in our high risk communication acts, we need to know are there just in case.

Grounded Theory model building

This section partially supports the model factors:

Information Usage (IU): Later IU – repeated viewing (Sub-section 8.3.4.3)

recording data increases its sensitivity by giving the *Information Receiver* more control over the data.

3.3.1 Reciprocity mechanisms in media spaces

Portholes is a system whose purpose is to develop a sense of awareness and social proximity amongst its remotely located users. The system presents a tiled view of media space members’ video snapshots that are updated every minute (see Diagram 3.1). With the introduction of video-cameras throughout offices, systems, such as portholes, take videoconferencing beyond a simple videophone analogy (Dourish & Bly, 1992). This technology can both vastly enhance group collaboration benefits and at the same time increase potentially serious privacy issues (Bellotti & Sellen, 1993; Bellotti, 1997).

Many media spaces have caused privacy concern for users with a lack of feedback about when an image is grabbed, what the image looks like and who is grabbing it. *Reciprocity*¹¹ has been noted as an essential element in CSCW communications. The majority of privacy mechanisms in media spaces have, therefore, concentrated on providing reciprocity e.g. allowing the user to monitor and control their self-presentation and behaviour, through feedback (Lee et al., 1997; Isaacs & Tang, 1997). The Ontario Telepresence Project included door state icons that relayed, to those viewing, the accessibility of group members (Buxton, 1997). The door state allowed for a restriction on the distribution of images. Since the images relayed are static and have no audio the privacy threat is less than someone looking through the window of an office door. However, I propose that someone glancing in an office door is a very different scenario, in privacy terms, from sitting in a chair staring through that same door (as with this media space). This is understood, to some extent, and reflected in media space applications that distinguish between the act of glancing and that of staring (Dourish, 1993; Isaacs & Tang, 1997).

A further argument suggests that privacy problems do not come from the different types of viewing actions but users’ awareness of being watched. Is anyone watching the watcher? It is argued that

reciprocity can again correct these privacy problems by increasing the notion of social norms within media spaces (Dourish, 1993; Bellotti & Sellen, 1993; Isaac & Tang, 1997). Many media spaces (Montage, Godard, Cavecat, Cruiser¹²) increase reciprocity by providing the office worker being glanced at visual or aural feedback that this eavesdropping is occurring. In other words those who are being watched, watch those *glancing* at them. However, there are no mechanisms that provide immediate feedback to those *glancing* that they too are now being looked at (see Diagram 3.4). To act as an effective inhibitor (thus reducing snooping and eavesdropping) the eavesdropper should also have immediate feedback that they have been seen watching the user. This in turn would change the act of glancing into one of opening the door and peering in, thus dissuading people from glancing at all. Ultimately the current notion of reciprocity within media spaces does not allow for the complexity of the social norms and pressure involved in containing our behaviours to those that are acceptable. When using a corridor it is understood that others use the corridor (C in Table 3.2 and Diagram 3.4) and thus the chances of someone viewing you glancing in through the window of a door is increased. As it is considered (within western societies) socially inappropriate behaviour to snoop, peep, look in on someone without his or her consent we feel a sense of social pressure against glancing in on someone (see Table 3.2 and Diagram 3.4). It is this pressure which contains inappropriate viewing behaviours that are not contained in many media spaces. In a media space the act of glancing in on a co-worker becomes a private interaction (reduced social pressure) in which only one user receives immediate feedback on being viewed (see Table 3.2 and Diagram 3.4).

B GLANCES IN ON A			
REAL WORLD		MEDIA SPACE (most?)	
Actions	Repercussions	Actions	Repercussions
1) A often does not see that B has seen them	(often not disturbed)	A sees that B has seen them	(disruption)
2) B may be viewed by C (a passer-by)	(feedback to C – the passer-by)	B does not realise that A can see them	(lack of feedback to B)
3) B sees that C (a passer-by) has seen them	(feedback to B social pressure on B)	C (other local users) does not know about A or B interaction	(glance now private – no social pressure)

Table 3.2: Real world and media space glancing behaviours

¹¹ The ability to know or see that someone is looking at you.

¹² Cruiser (Root, 1988), Cavecat (Milligan, 1991), Rave (Gaver et al, 1992), Godard (Dourish, 1993), Montage (Isaacs & Tang 1997), Nynex (Lee et al , 1997)

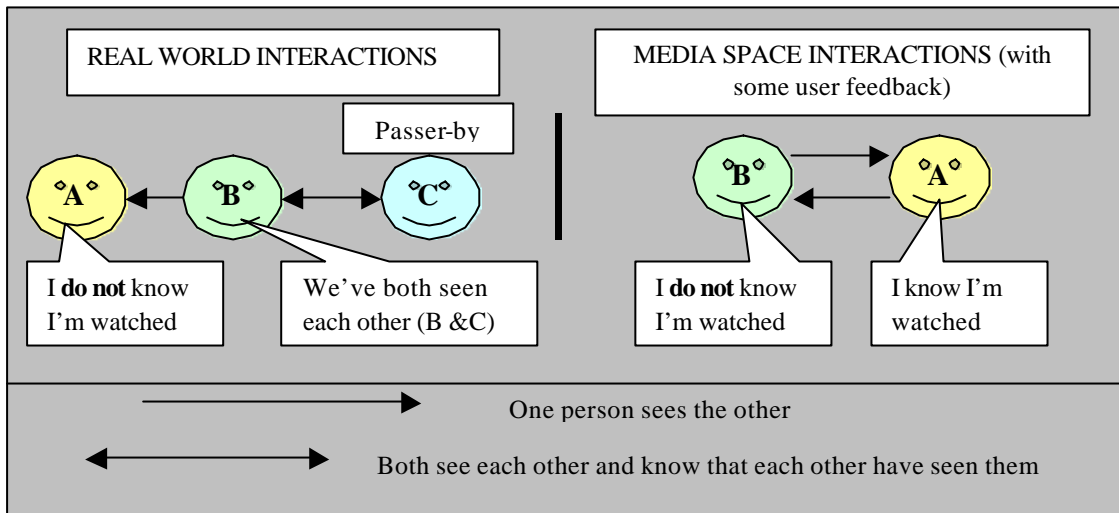


Diagram 3.4: Real world and Media space glancing behaviours

Grounded Theory model building

This section partially supports the model factors:

IR: Trade-off's – trust (Sub-section 8.3.3.3) and reciprocity

IU: Later IU – recording awareness (Sub-section 8.3.4.2) with regard to feedback

Context: Technology – interface issues (Sub-section 8.3.5.2)

Context: Technology – presence (Sub-section 8.3.5.3) and awareness

3.3.2 Anonymity and control

Mackay (1995) noted in her suggestions for ethical video-taping and its usages that individuals identity should be hidden, where-ever possible. The connection between identification and privacy is founded in the data-centric perspective of privacy (see Sub-section 2.2.2). It may seem absurd to anonymise data in an environment that concentrates on identifying the individual but many privacy mechanisms have sought to give the user the control over their image transmission through anonymising it.

Awareness technologies have been key in the movement to provide awareness to co-workers, that users are around and available to collaborate, while retaining their privacy through anonymising the details of their specific actions and with whom. Smith & Hudson (1995) identified 2 problems with audio media space - awareness technologies (shared audio channel – everyone hears the speech on the channel):

- 1) Disturbance from audio feedback caused users to turn it off and forget to turn it back on again.
- 2) If distribution were not fully understood by the user they would resort to other communication channels for sensitive communications (Smith & Hudson, 1995)

To resolve these privacy problems an audio processing technique was devised which was less demanding of the listeners' attention than actual speech and yet preserved the privacy of the speaker by masking full conversations. This allowed knowledge of users' presence to be conveyed without allowing others to overhear every word being spoken. Users' related concerns about image details being transmitted within the media space NYNEX (Lee et al., 1997) were similarly counteracted by a mechanism which allowed users to alter the degree of image clarity (normal, foggy, grey, black).

What seems to emerge from these examples is that many users' privacy worries in media spaces have centred on their control of data transmission and distribution. Smith and Hudson (1995) go further and suggest that to retain privacy a clear distinction is required between the sending and receiving user whereby the former requires control of what data is released. Many application designers originally stated that users could control image transmission by pointing their camera at the wall or out the window (Dourish, 1993; Lee et al., 1997). However many applications introduced a more usable door mechanism which would allow users to pre-state who could view them and in what way (glance, portholes view, videophone etc). 'Montage' offers a *do not disturb* mode that blocks incoming glances (Isaacs & Tang 1997).

Despite an understanding by many media space designers that user control and anonymity is important in retaining privacy there has been a move to automate many aspects of these applications. Some users have objected to the lack of control they have over their images with automatic capture of images (Lee et al., 1997). Cranor et al. (1999) also established that users consider automated data capture a major cause of privacy invasion. I would propose that it is the automatic construction of information out of data that causes potential privacy invasions rather than merely automating mechanisms. The NYNEX system, for example, automatically presents users' precise activities anonymously by only presenting a bar chart of the degree of activity in images over a 12 hour period. This enables the viewer to identify when the user is busy and active and when not (Isaacs & Tang 1997). Greenbergs' (1996) *peepholes* application similarly has iconic presence indicators, instead of video, to show the availability of people in a virtual community. The computer automatically captures and transmits data on activity patterns (currently active on the computer, computer idle, computer idle a long time, logged off the computer, unreachable). The application also automatically informs the user if someone has become active by playing an audible sound of someone typing. Automatically translating *activity data* into information could distort the original data. Both of these applications, although providing the user with a degree of anonymity, could be potentially invasive by presenting daily activity patterns in a simplified format (e.g. 'Johns looks like he's been a bit slack in working today). These arguments relate back to those presented in Section 2.1 of the importance of data context (see Sub-section 2.3.3).

Grounded Theory model building

This section partially supports the model factors:

User factor: user distinction (Sub-section 8.3.1.2) distinction between sending and receiving user.

Context: Technology – environments (Sub-section 8.3.5.1)

Context: Technology – interface issues (Sub-section 8.3.5.2)

Context: Technology – presence (Sub-section 8.3.5.3)

3.3.3 Platform for privacy preferences (P3P)

The platform for privacy preferences (P3P) aims to enable users to apply preferences over privacy practices at the web site. Although P3P does not specifically relate to multimedia communications there could be some technical implications for this field. Ultimately P3P provides a technical mechanism for ensuring that data is released only under an acceptable agreement. Initially the web-site sends a proposal of its privacy practices, which is compared against the users' predefined preferences (Reagle & Cranor, 1999). To reduce user effort the proposal can be automatically parsed and compared with the users' preferences by a semi-autonomous agent (Ackerman & Cranor, 1999). However, there is still time and effort involved in initially defining the preferences. Cranor & Reagle (1998) argue that the solution to this problem is well-defined layered interfaces providing users with choice in preference setting. For these interfaces to be effective, though, they should be based upon a detailed and accurate model of how users perceive privacy. Unfortunately this research knowledge does not exist especially within the field of multimedia communications.

The P3P mechanism often highlights that a third party service, such as TRUSTe (Benassi, 1999), assures that the company keeps within certain guidelines. However, the usefulness of these third party services depends upon how much the user trusts them. The virtual isolation of many of these organisations (i.e. they only exist in the virtual world) decreases the likelihood of novice users trusting them. The use of brand or real world organisational names linked to trust badges could reduce these problems e.g. Visa, trading standards, government bodies (Reagle & Cranor, 1999).

A further problem with this approach, identified by this thesis, is that it is based upon the traditional paradigm's data-centric perspective of privacy. Guidance of potential privacy threats and useful feedback required for trade-offs is not provided for the user. Data is also viewed in a data-centric way with highly sensitive information directly relating to personally identifiable data and the extent to which that data is distributed. This approach does not allow for individual variations and trade-offs that users may want to make.

Grounded Theory model building

This section partially supports the model factors:

P3P relies on the users' preference with regard to information receivers and usage

Information Receiver: Trade-off's – trust (Sub-section 8.3.3.3)

Information Receiver: Trade-off's – roles (Sub-section 8.3.3.4)

Information Usage (IU): Current IU – task (Sub-section 8.3.4.1)

Information Usage (IU): Later IU – repeated viewing (Sub-section 8.3.4.3)

Information Usage (IU): Later IU – editing (Sub-section 8.3.4.5)

Trust and common norms with virtual organisations in paramount

Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

Context: Organisational culture – trust (Sub-section 8.3.5.7)

3.4 PRIVACY APPROACHES IN MULTIMEDIA COMMUNICATIONS.

To devise effective solutions to privacy problems within multi-media communications there is a need to identify a model of users' perceptions within this domain. This model should establish factors involved in determining privacy levels before systems are developed so that privacy is dealt with pro-actively rather than retrospectively, as has been the case in the past (Smith, 1993).

There have been two major approaches that have affected research into users' perceptions of privacy in multimedia communications both of these will be reviewed in this Section. Privacy has been noted as being especially important in the ubiquitous computing environments of multi-media communications. Bellotti & Sellen (1993) argue that it is the ubiquity of unobtrusive technology that increases the risk of privacy invasion by providing more data with less control and feedback to users. Within HCI privacy research the control and feedback perspective has been the main direction for privacy reviews. Recent research has, however, identified a second perspective noting the importance of context in users' perceptions of privacy (Harrison & Dourish, 1996).

3.4.1 Control and feedback approach

Over the past decade there has been a move to define privacy within the computer domain in more detail. Stone et al. (1983) suggested the importance of the individuals' ability to control data about themselves. Bellotti (1996) refers to this as the *operational* privacy definition (see Sub-section 2.2.3) which reviews users' capabilities to retain privacy via access control and feedback. It is argued that if these factors (see Table 3.3) are considered in systems design deployment and use then privacy intrusions would greatly be reduced.

Control	Empowering people to stipulate what data they project and who can get hold of it
Feedback	Informing people when and what data about them is being captured and to whom the data is being made available

Table 3.3: Defining control and feedback

The clear advantage of this approach is that it relates users' privacy rights to technical and interface design decisions. With careful privacy related design, users should have increased control of personal data and thus privacy (Bellotti & Sellen, 1993). This, in effect, will produce self-regulation of potential privacy invasions. It is suggested that feedback and control should be integrated into systems dependent on certain types of users and system behaviours (Table3.4)

Capture	What kind of data is being picked up; voice, work activity & products such as key presses
Accessibility	Who has access to the data
Purpose	To what use is the data put
Construction	What happens to the data ... kept and manipulated out of context.

Table 3.4: Behaviours affecting control and feedback mechanisms (Bellotti & Sellen, 1993)

However, these findings do not identify the interactions between these categories - if they exist. For example, who is likely to use the data may effect its level of sensitivity - this would effect the type of mechanisms that are devised with sensitivity levels varying for differing users and usages.

Although Bellotti & Sellen (1993) suggest that it is dangerous to rely on social and organisational controls of *Personal Information*, or trade-off's for perceived benefits 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. Bellotti & Sellen (1993) have, however, related *Information Usage* to the context in which those who receive it act upon it - be it another user or the organisation. This is done by identifying potential privacy problems using data out of context by:

1. *Disembodiment* with the context resulting from a lack of *control* and *feedback*.
2. *Dissociation* from ones' actions due to a lack of *control* and *feedback*.

Bellotti (1996) also proposes that there is an argument for another area of debate in the users' access to, and sharing of data. The main criteria for ensuring systematic evaluation of system solutions to incorporate effective feedback and user control can be seen in Table 3.5.

1	Trustworthiness	technically trustworthy systems
2	Appropriate timing	timely feedback
3	Perceptibility	noticeable feedback
4	Unobtrusiveness	don't overload user with feedback
5	Minimal intrusiveness	reduced privacy invasion for others
6	Fail-safety	increased privacy for defaults
7	Flexibility	adaptable to context & interpersonal relationships
8	Low effort	reduced user input
9	Meaningfulness	feedback should be information not data
10	Learnability	usable & user-friendly
11	Low cost	Economically viable

Table 3.5: Criteria for privacy system solutions (Bellotti, 1996)

One serious shortcoming of the control and feedback approach to privacy, identified by this thesis, 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. Furthermore, this approach does not consider the complexity of the privacy problem. Interactions between privacy factors may seriously affect users' judgements with reference to privacy invasion. Finally, as has been mentioned throughout this thesis, the importance of the trade-off's users make in certain situations and contexts must not be underestimated. To define privacy adequately, it must be understood that this it is an unstable phenomenon that varies according to context, users' roles and societal and organisational norms whilst privacy benefits can affect users' overall perceptions (Dourish, 1993; Bellotti & Sellen, 1993; Bellotti, 1997).

Grounded Theory model building

This section partially supports the model factors:

Information Usage (IU): Current IU – task (Sub-section 8.3.4.1) disembodiment, dissociation.

Information Usage (IU): Later IU – recording awareness (Sub-section 8.3.4.2) and appropriate feedback.

Information Usage (IU): Later IU – context (Sub-section 8.3.4.4): what released

Information Usage (IU): Later IU – editing (Sub-section 8.3.4.5): how used.

Context: Technology – interface issues (Sub-section 8.3.5.2) control and feedback

3.4.2 Context approach

Kling (1987) suggests that mechanistic approaches to information systems focus just on economic, physical and data processing aspects of the technology. The context of complex social actions in which these systems are developed is ignored. When designing computer systems usability should not be confused with acceptability for as Harper (1992) points out;

“ The fact that something is practical does not of course ensure that it is acceptable.” (p.332).

There have been three specific issues highlighted with respect to the effects of context on privacy in multimedia communications. Firstly the users’ perceptions of situation, secondly their role within the organisation and finally the organisational culture within which the technology is embedded (Adams, 1999a; Adams & Sasse 1999a &b).

Harrison & Dourish (1996) argue that it is a *sense of place* that guides social interactions and our perceptions of privacy rather than the physical characteristics of a space. We expect different behaviour in private and public situations. This is because social norms guide our perceptions of spaces allowing us to interpret them as places and adapt our behaviours accordingly. All parties within the same culture understand what is and is not acceptable in a given situation (i.e. it is acceptable to stare at a street performer but not at a passer-by). However, our perception of a situation also depends on how we see ourselves in that situation (Goffman 1969). Ultimately, how we perceive ourselves depends on assumptions made about a situation that are based on social norms. Complex variations in users’ perceptions of a situation could be a potential problem in privacy design. A situation considered public to one person may be equally considered private or semi-private to another. It is argued by this thesis, that the importance of these issues within multimedia communications requires further investigation.

Harper (1992) proposes 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 their state of relations with others. Applications, which merely preserve and reflect the already existing status quo of data distribution and usage will be more acceptable than those that change the character of their relations with others. Again I would propose that these issues have not been fully investigated within the specific domain of multimedia communications.

Finally, it has been argued that technology is situated within a culture which determines aspects of its use. The relationship between technology and its use is co-adaptive (Dourish, 1993; Harrison & Dourish, 1996). Certain technologies may apply well in an environment of trust but fail in an atmosphere of distrust. Within specific organisational cultures fewer privacy protocols are required as social norms protect users’ privacy. The media space at Xerox PARC operated on a ‘sign-up’ basis whereby those that opted into the application were considered to accept the social practices and norms which govern acceptable use of the space (Dourish, 1993). However, I would argue that this assumes

privacy invasions only occur through *intentional* acts of inappropriate behaviour. Ultimately, although context is a vital element in users' privacy perceptions the issues are far more complex than organisational trust. I propose that an attempt to identify all of the relevant basic elements of users' privacy perceptions is needed so that further research may detail context-specific variations.

Grounded Theory model building

This section partially supports the model factors:

Information Sensitivity: Public / private situation (Sub-section 8.3.2.2)

Information Receiver: Trade-off's group membership (Sub-section 8.3.3.5)

Context: Social groupings – social groups (Sub-section 8.3.5.2)

Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

Context: Organisational culture – trust (Sub-section 8.3.5.7)

Context: National and international – cultural norms (Sub-section 8.3.5.8)

3.5 CHAPTER SUMMARY

HCI research has reviewed various multimedia environments and identified that packet loss, virtual environments, media spaces and portholes have specific privacy implications (see Section 3.1). The location of technology, accessibility of data, users' perceived anonymity and virtual cultures are also all important multimedia communication privacy issues (see Section 3.2). HCI researchers have proposed that reciprocity and increased user control & feedback are the basis for privacy protection mechanisms to solve media space privacy invasion problems (see Section 3.3 & Sub-section 3.4.1). However, recently HCI research has noted that context is also an important approach to privacy in multimedia communications - specifically users' perceptions of situation, their role within the organisation and the organisational culture. (see Sub-section 3.4.2). Ultimately privacy is a complex phenomenon that must be evaluated from the users' perspective to identify core issues on which to develop appropriate privacy protection mechanisms and organisational policies.

A Grounded Theory summary of research from this chapter is presented in Table 3.6. This representation shows how the research presented in this chapter expands the privacy model being developed, where the gaps are currently in the model and how the following chapter will expand on the model.

Model Factors	Chapter 3 Privacy model contributions	Building on Chapter 2 & Gaps in the model	Chapter 4 Model development
USER FACTORS		This research reviews system interaction but not privacy with user distinctions & mental models.	The following chapter will present arguments behind a Grounded Theory approach to developing a model of users' perceptions of privacy within multimedia communications that builds upon this research and fills in some of the gaps.
<i>System interaction</i>	Section 3.2		
INFORMATION SENSITIVITY (IS)		This research builds on situation research (Chpt. 2) but not information's perceived primary and secondary levels or trade-off's made.	
<i>IS Judgements</i>	Sub-section 3.2.2		
<i>Public / private situation.</i>	Section 3.2 and Sub-sections 3.2.2, 3.4.2	This HCI research builds on previous (Chpt 2) information receiver issues such as trust, but there is no HCI overview of privacy implications between and across multimedia communication <i>environments</i> .	
INFORMATION RECEIVER (IR)			
<i>Trust</i>	Sub-sections 3.2.1, 3.4.2		
<i>Relationships</i>	Sub-section 3.2.1		
<i>Trade-off's – trust</i>	Sub-sections 3.2.1, 3.3.1, 3.3.3, 3.4.2		
<i>Trade-off's – roles</i>	Sub-section 3.3.3		
<i>Trade-off's – group membership</i>	Sub-sections 3.2.1, 3.2.2, 3.4.2	HCI privacy research reviews information usage issues which previous interdisciplinary research overlooks (Chpt.2). This research, however, inclines towards technical mechanisms for solutions and not users' perceptions of these factors or how trade-off's are made.	
INFORMATION USAGE (IU)			
<i>Current IU – task</i>	Sub-sections 3.2.2, 3.3.3, 3.4.1		
<i>Later IU – recording awareness</i>	Sub-sections 3.2.1, 3.2.2, 3.3.1, 3.4.1		
<i>Later IU – repeated viewing</i>	Sub-sections 3.3, 3.3.3		
<i>Later IU – context</i>	Sub-sections 3.2.2, 3.4.1, 3.4.2		
<i>Later IU - editing</i>	Sub-sections 3.2.2, 3.3.3, 3.4.1	HCI research builds upon previous findings into context and privacy (Chpt.2) and extends this to include application specific reviews of environments and interface issues. There is, however, no HCI overview of the privacy implications between and across multimedia communication <i>environments</i> .	
<i>Later IU – trade-off's risk/benefit</i>	Sub-section 3.4.2		
CONTEXT			
<i>Technology – environments</i>	Sub-sections 3.1.1, 3.1.2, 3.1.3, 3.2.2, 3.3.2, 3.4.2		
<i>Technology – interface issues</i>	Sub-sections 3.2.2, 3.3.1, 3.3.2, 3.4.1		
<i>Technology – presence</i>	Sub-sections 3.2.1, 3.2.2, 3.3.1, 3.3.2, 3.4.1		
<i>Social groupings – social groups</i>	Sub-sections 3.2.1, 3.3.1, 3.3.2, 3.4.2		
<i>Social groupings –outsiders</i>	Sub-section 3.2.1		
<i>Organisational culture –norms</i>	Sub-sections 3.3.3, 3.4.2		
<i>Organisational culture – trust</i>	Sub-sections 3.3.3, 3.4.2		
<i>Nat/international – cultural norms</i>	Sub-sections 3.2.1, 3.4.2		

Table 3.6: Grounded Theory summary of HCI specific research, model contributions and gaps

Chapter 4: Methodology

Human computer interaction (HCI) is a discipline requiring a knowledge base that reflects its interdisciplinary nature. The relatively short history of this discipline, however, has not enabled it to build a detailed multidisciplinary knowledge base to reflect its specific nature. Research within this discipline should, therefore, seek to increase the knowledge base whilst building upon existing information.

4.1 HCI AS A RESEARCH DISCIPLINE

The aim of HCI research is to construct a knowledge base that will aid designers in the building of usable computer systems (Preece et al., 1994; Cockton, 1999). The domain requires both substantive and methodological knowledge that will be both accessible and applicable for designers. This thesis seeks to build upon relevant knowledge from related disciplines and HCI (see Diagram 4.1).

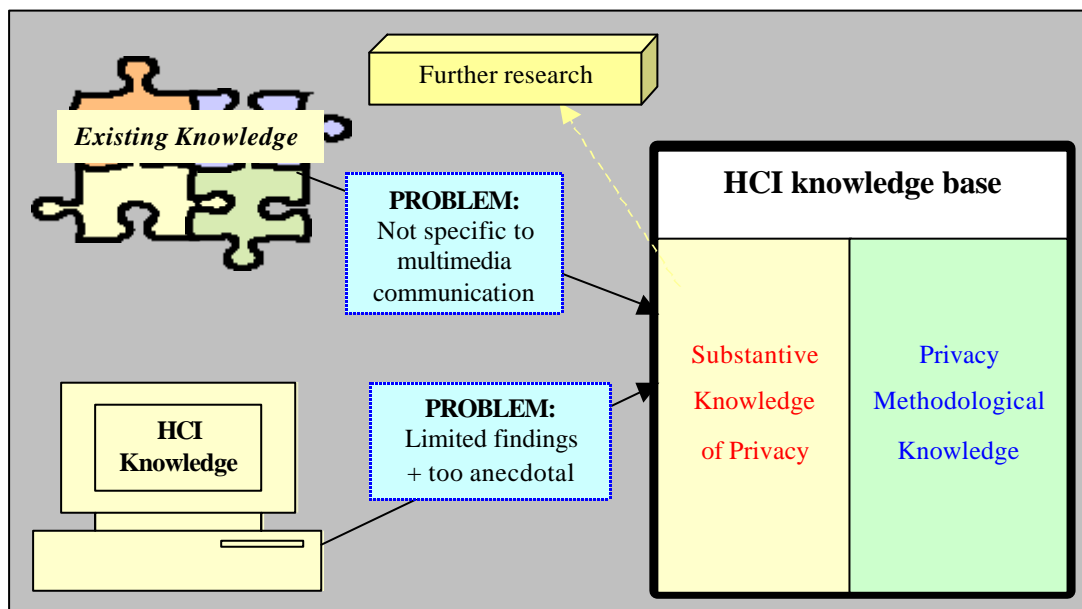


Diagram 4.1: Input to HCI knowledge base

However, it is important to identify the limitations of previous research when investigating users' perceptions of privacy within the specific field of multimedia communications. Existing privacy knowledge (psychological, sociological, legal), although providing insightful into the complexity of users' perceptions of privacy, does not:

- relate to HCI knowledge on multimedia communications;
- translate directly into knowledge that will aid designers in building usable computers;

Current HCI knowledge on privacy, although relating to computers and multimedia communications, is:

- mostly anecdotal rather than scientific;
- the scientific knowledge currently available is system-specific with poor generalisability to aid designers within different contexts. Much of the current HCI privacy research increases privacy, via mechanisms, for a specific application within a specific context (e.g. *Montage, Godard, Cavecat, Cruiser*¹³). This negates the importance of changes in context such as task, organisational setting and participants that could have a dramatic effect on the mechanisms effectiveness (see Chapter 3).

These limitations suggest that further scientifically based, structured research within multimedia communications is required (see Diagram 1). This thesis seeks to develop a descriptive model of users' perceptions of privacy in multimedia communications providing testable theories and guidelines for application designers. This model will, therefore, inform the HCI substantive knowledge base whilst new methodologies for researching this complex phenomenon will inform the HCI methodological knowledge base.

4.1.1 HCI research approaches

Sasse (1997) identifies three principal approaches to HCI research. These approaches are reviewed for their applicability with this thesis in mind.

1. Scientific approach (Newell & Card, 1985).
2. Craft-based / design-science approach (Carroll & Campbell, 1989).
3. Engineering approach (Dowell & Long, 1989).

The scientific approach seeks to provide knowledge through scientific models and approximate calculations (Newell & Card, 1985). HCI problems are solved scientifically using *priori-theory*¹⁴ (see Sub-section 4.2.1) methodologies for applicable cognitive psychology knowledge. Substantive knowledge of lower-level cognition within psychology relates to phenomena such as perception, attention, motor control and memory capacities (Wickens, 1992; Preece et al. 1994). There are, however, three major problems with the scientific approach for this research project:

- 1) As privacy is a complex high-level phenomenon, which is currently not well understood, a traditional scientific approach using only quantitative measurements and calculations would be inappropriate. This phenomenon requires an explanatory, conceptual HCI research approach.

¹³ Cruiser (Root, 1988), Cavecat (Milligan, 1991), Rave (Gaver et al, 1992), Godard (Dourish, 1993), Montage (Isaacs & Tang 1997), Nynex (Lee et al , 1997)

¹⁴ *Priori-theory* is the basis of traditional experimental research whereby research is conducted to prove or disprove a theory or hypothesis, which is chosen prior to the study being conducted. This is sometimes termed hypothesis testing (Henwood and Pidgeon, 1992).

- 2) The findings of this thesis should relate back to designers as prescriptive knowledge. It is argued that the traditional scientific approach does not fulfil this requirement which is why few designers have taken up science-based modelling techniques (Bellotti, 1988; Dowell & Long, 1989).
- 3) Science-based knowledge acquisition requires costly data collection procedures which would not allow for a *privacy model* to be developed ethically within the time-constraints provided.

The craft-based approach proposed by Carroll & Campbell (1989) advocates conceptually deep (containing theoretical context specific abstract relationships), explanatory HCI theories (in the form of heuristics) acquired experientially (by practice and example). This approach, therefore, provides designers with HCI knowledge that is relevant and immediately applicable to individual design needs (Carroll & Campbell, 1989). Again, however, this approach is limited in its applicability for this thesis. The main argument against this approach is that it remains an informal, *anecdotal science* which cannot be verified or generalised (Long & Dowell, 1989). Although the craft-based approach appropriately emphasises the importance of contextual issues in producing valid and applicable research results it has also restricted current privacy in multimedia communication research to application-specific findings.

Finally the engineering approach seeks to accumulate knowledge and formulate engineering principles as a foundation for HCI design and evaluation. This approach views the user as a component of the overall system and seeks to take knowledge which is codified, formal and operational and present it as HCI knowledge in the form of engineering principles that are prescriptive, and accessible by designers (Dowell & Long, 1989). However, the complexity of the privacy phenomena and lack of previous research require an approach that is more conceptually deep and explanatory in its foundations than this approach would allow.

Ultimately this thesis requires an approach which can :

- Build HCI theory (despite little previous research) which is empirically based and systematically developed.
- Integrate current interdisciplinary knowledge into the theory.
- Deal with the complex nature of the phenomena (i.e. user perceptions, privacy).
- Provide designers with accessible and applicable multimedia communication privacy guidance.

The nature of this phenomenon advocates a qualitative approach, although the requirements of the HCI knowledge base imply that a systematic quantitative approach is required. For the purposes of this thesis the post-positivistic Grounded Theory methodology fulfils both of these requirements (see Section 4.2). Current HCI advances in grounded design are foremost for this thesis approach to the application of Grounded Theory within the HCI paradigm (Cockton, 1999; Clarke & Cockton, 1999).

4.1.2 Qualitative HCI research

As much of the research within HCI seeks to inform designers in a structured, applicable way, qualitative research has, to-date, been the poor relation of the experimental approach. However, there are many complex, socially based phenomena in HCI that cannot be expressed by an engineering-style or traditional science approach. Other approaches, therefore, to constructing non-mathematical theories have to be considered within HCI.

Social science methodologies have been used for some years in HCI particularly in the field of computer supported collaborative work (CSCW: Suchman, 1987; Fafchamps, 1991). However, these studies tend to be restricted to observational, ethnographic style research limiting their prescriptive abilities. Some of the research has taken a more empirical approach with methodologies such as conversational analysis (Bowers, Button & Sharrock, 1995; Bowers, Pycock & O'Brian, 1996; Hindus, Ackerman, Mainwaring & Starr, 1996). However their effectiveness in theory building is very limited. Ultimately a more focused and structured approach to HCI qualitative research is needed that will provide theories and applied models based on both qualitative and quantitative data.

The research focus of this thesis deals with a phenomenon that is complex and yet has little previous applicable substantive knowledge (see Chapter 3) upon which to base further research. Through Grounded Theory analysis (see Section 4.2) of this phenomenon, this research will provide (for multimedia designers needs):

1. a theory of users' perceptions of privacy in multimedia communications;
2. guidance for effective user privacy protection design in multimedia communications;
3. guidance for further privacy research within multimedia communications.

Grounded Theory model building

This section partially supports the methodological issues:

Phenomena complexity (Sub-section 10.2.3)
Theory building & Integrating mixed data (Sub-section 10.2.4)
Structured / focused approach (Sub-section 10.2.2)

4.2 RESEARCH METHODOLOGY: GROUNDED THEORY

Grounded Theory is applicable for this research because of its hierarchical nature, with process effects connecting concepts, and its context specificity while still remaining scientifically based. Because of these advantages Grounded Theory was used in this research:

- i) To help define the scope and structure of this thesis.
- ii) At a high-level to allow for both previous and thesis research findings to feed into the privacy model.
- iii) At a low-level as a methodology and analysis tool for all the thesis research studies.

4.2.1 Grounded Theory

Unlike other social science methodologies, Grounded Theory (Strauss & Corbin, 1990) provides a more focused, structured approach to research (closer in some ways to quantitative methods) which is why it has been termed a post-positivistic method (Stevenson & Cooper, 1997).

Grounded Theory was originally identified as the product of close inspection and analysis of qualitative data (Glaser & Strauss, 1967). Later Strauss & Corbin (1990) used the term to refer to a data collection and analysis technique that they formulated which was no longer restricted to qualitative data. Grounded Theory is an alternative approach to data collection and analysis that combines various systematic levels of abstraction into a framework about a phenomenon which is verified and expanded throughout the study.

“The research findings constitute a theoretical formulation of the reality under investigation, rather than consisting of a set of numbers, or a group of loosely related themes.” (Strauss & Corbin, 1990, p.24)

Successful application of the methodology is assessed in terms of the final account’s comprehensiveness and *fit* with the data. Strauss & Corbin (1990) suggest that Grounded Theory is especially useful for complex subjects or phenomena where little is yet known. 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.

Grounded Theory uses data, gathered by a variety of different means, which is analysed using a non-mathematical procedure. Qualitative or quantitative data can be used by the analysis which does not require a prior hypothesis for focusing (Strauss et al, 1964). This then allows research data previously collected on the same phenomena to be used for further research. Although there is flexibility in the type of information used for Grounded Theory analysis a greater emphasis is placed on the subject sampling and contextual considerations so that later transferability of findings can be increased.

Once the data is collected it is analysed in a standard Grounded Theory format (for coding examples from studies 1-5 see Appendix 1). Data, in whatever form, is broken down, conceptualised and put back together in new ways. To enable this to occur in a structured manner Strauss & Corbin (1990) have devised 3 major coding stages (open, axial and selective) in the analysis procedure. It must be acknowledged, however, that the lines between these forms of coding are artificial as is the divide between data collection and analysis. All of these elements are tightly interwoven in a complex structure of analysis and verification.

The *open coding stage* identifies concepts pertaining to similar phenomena (categories) along with identifying the properties and dimensions of the said category.

1. Concepts are identified.
 - *Concepts are* :- Conceptual labels placed on discrete happenings, events, and other instances of phenomena
2. Concepts are compared to see if they pertain to a similar phenomenon (category).
 - *Categories are* :- where concepts are classified and grouped together under a higher order – a more abstract concept called a category.
3. Identify the properties and dimensions of the category (see Table 4.1).
 - *Properties (Attributes) are* :- characteristics pertaining to a category
 - *Dimensions (Domains) are*:- Location (values) of properties along a continuum

Category Class	Properties Attributes	Dimensional Range (Domain)
surveillance	frequency	oftennever
	scope	moreless
	intensity	high.....low
	duration	longshort

Table 4.1: Example of a category broken down into properties and dimensions

Axial coding then identifies the high level phenomena (e.g. central ideas, events) along with the conditions and participants strategies pertaining to those phenomena (e.g. causal conditions, intervening conditions).

1. Key high level phenomena are identified
 - *Phenomena are*:- central ideas, events.
2. Conditions pertaining to those phenomena are identified. These are namely the causal condition, context of the phenomenon & any intervening conditions.
 - *Causal conditions are*:- events that lead to occurrence or development of a phenomenon.
 - *Context*:- The *specific set of properties* that pertain to a phenomenon, locations pertaining to a phenomenon along a dimensional range.
 - *Intervening conditions*:- broader structural context
3. Identify any action / interaction strategies that are produced in response to the phenomena
 - *Action / interactional strategies*:- devised to manage, handle, carry out, respond to a phenomenon under a specific set of perceived conditions
4. Identify any Consequences from these A/I strategies.
 - *Consequences*:- Outcomes or results of action / interaction

For example:

“ When I want to have (context) a personal conversation (phenomenon), I encrypt the message (strategy). I think that makes the email private (consequence).”

Finally the analysis is elaborated upon and interpreted in the *selective coding stage*. The core category (the central phenomenon around which all the other categories are integrated) is defined here and a conceptualisation of the descriptive narrative, set around the core category, is exposed. This whole process is iterative so that it is validated by continual comparisons with the raw data to confirm or refute conclusions. This continual validation can produce gaps in the framework that can only be filled in by further research.

1. Define the core category and a high-level story line

The story-line is set around the core category which defines the whole

- *Core category is:* The central phenomenon around which all the other categories are integrated
- *Story is:* A descriptive narrative about the central phenomenon of the study
- *Story line is:* The conceptualisation of the story - the core category

2. Relating the subsidiary categories around the core category by means of its properties.

- This is best done with graphical representations of the core category and subsidiary categories. The core category properties are high level definitions

3. Relating categories at the dimensional level

- This then ties up in detail, finally all the categories into a whole model / framework which is defined by the story-line and the core-category.

4. Validating relationships against data

- The process of building the core-category and story-line is an iterative process which is validated by continual comparisons with the raw data to confirm or refute your conclusions.

5. Filling in categories which need further refinement

- Often after defining some categories gaps appears in the high-level story-line which can only be filled in by further research.

The last stage in the analysis is the integration of *process effects* (e.g. factors changing over time) so that changing factors within the framework can be identified.

Define any process effects that may be occurring

- *Process is:-* the linking of action-interaction sequences over time (see Diagram 4.2)

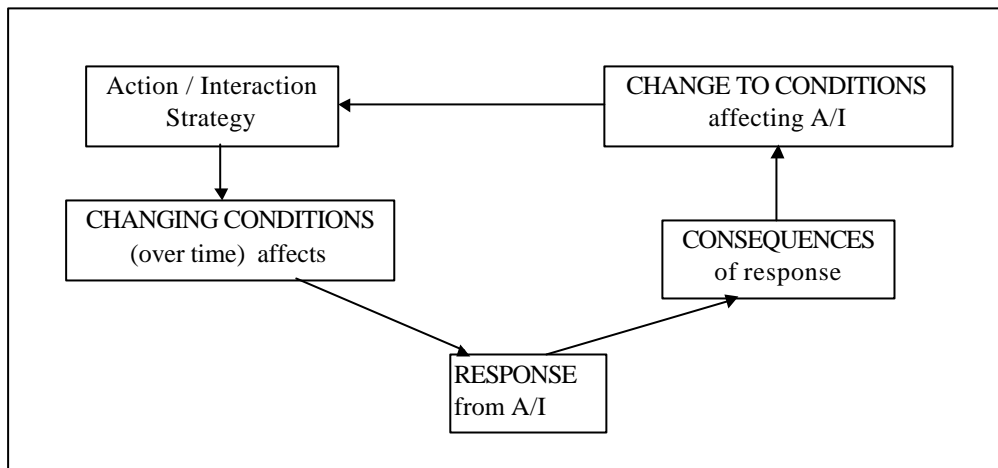


Diagram 4.2: Graphical representation of a process effect chain

Grounded Theory model building

This section partially supports the methodological issues:

Phenomena complexity (Sub-section 10.2.3)
Structured / focused approach (Sub-section 10.2.2)
Integrating mixed data (Sub-section 10.2.4)

4.2.2 Grounded Theory applied to HCI research

HCI often needs to review complex phenomena and develop applicable frameworks for action yet due to its short history it has not yet established an extensive knowledge base on which to base its research. Ultimately HCI research requires the in-depth nature of qualitative research to review these complex phenomena with the structure of quantitative research. Over recent years, however, the debate between the quantitative and qualitative paradigms has become very heated (Morgan, 1996; Sherrard, 1997; Stevenson & Cooper, 1997). Henwood & Pidgeon (1992) argue that the debate should move away from this destructive approach and concentrate on identifying criteria for good research in all its formats.

The goal of both qualitative and quantitative research paradigms is to build relevant, applicable theories (Henwood & Pidgeon, 1992). Ultimately, it is the structured approach to theory generation that is pivotal within Grounded Theory. The philosophy of science is based on the distinction between a *context of discovery* and a *context of justification*. Previous scientific methodologies have, however, concentrated on techniques within the *context of justification* rather than *discovery*. Within the field of HCI the *discovery* stage of research has been implicitly and explicitly noted as involving craft qualities. Although *priori-theory* in the scientific paradigm is usually based on previous research, at some point a researcher generates this theory in an unstructured manner. In a new field of exploration there must be an increase in this unstructured approach to the discovery stage as there are fewer relevant papers to look to for assistance. Henwood & Pidgeon (1992) argue that the *discovery* stage is a fundamental role in the scientific process. It could be argued that it is even more fundamental within the design procedures of HCI. Developing theoretically informed explanations is the most powerful way to

highlight reality. Building theory, it is argued, implies interpreting data, by its very nature, for the data must be conceptualised and the concepts related to form a hypothetical rendition of reality. The rendition that results cannot only be used to explain that reality but also to provide a framework for action within that context.

Grounded Theory model building

This section partially supports the methodological issues:

Phenomena complexity (Sub-section 10.2.3)

Theory building & Integrating mixed data (Sub-section 10.2.4)

4.2.3 Grounded Theory and the quality of research

There are several general arguments that have been presented to disclaim the usefulness of a Grounded Theory approach. It has been argued that this type of research lacks repeatability (Morgan, 1996). Repeatability is used to verify that findings can be generalised to other participants in similar situations. Strauss & Corbin (1990) argue that as long as the data used is comprehensive and the interpretations made are conceptually broad, the theory developed should be abstract enough and include sufficient variation to enable its application to a variety of differing phenomena related contexts.

The subjective elements of Grounded Theory have also been criticised. However Sherrard (1997) argues that the apparent lack of opinion within science is merely the product of avoiding socially controversial issues. Many of the research projects in HCI would be difficult to approach purely experimentally either because it would be unethical or because of the complexity of the issues involved. It is also argued (Henwood & Pigeon, 1992; Sherrard, 1997; Stevenson & Cooper, 1997) that subjectivity and bias are apparent, in varying degrees, in all research. The move, it is suggested, should therefore be to acknowledge these biases for scrutiny by professional counterparts, rather than denying that they exist. Henwood & Pidgeon (1992) suggest that all good quality research should provide documentation of the analytic process and a reflexive account of researchers' research backgrounds and perspectives. They also detail seven rules that should be followed to increase the quality of Grounded Theory research. To ensure a high standard of analysis Henwood and Pidgeons' (1992) quality rules were applied as a guidance in quality for all the studies in this thesis:

1. A constant comparison method was used as an internal check on validity ensuring that the framework developed retained the *importance of fit* to the raw data. (see Appendix 1, Study 1, Selective coding)
2. Multiple testing of hypotheses resulted in identification of relationships that were integrated at all levels of abstraction. (see Appendix 1, Study 2 & 3, Selective coding)
3. Increased validity of the research was obtained by endeavouring to increase its *Theoretical Sensitivity* using previous research comparisons. (see Tables 2.6, 3.6, 4.2, 5.3, 6.2, 7.5)

4. A *Theoretical Sampling* decision was made to use different multimedia applications (VC & VR) to allow for elaboration of the model and increase the conceptual depth of the analysis. (see Sub-sections 5.1.1, 5.2.1, 5.3.1, 6.1.1, 7.1.1)
5. An account of the contexts in which the studies were completed is provided. This increases the transferability of the findings to other contexts. (see Sub-sections 5.1.1, 5.2.1, 5.3.1, 6.1.1, 7.1.1)
6. Detailed documentation of the research process was taken and a sample of the process is provided (see Appendix 1).
7. To obtain *reflexivity* an account of the author's attitudes and approaches to research in general is provided (see Appendix 1)

Finally, because of the complexity in applying Grounded Theory appropriately, researchers' experience levels will alter the level of quality in the analysis and also the degree of subjectivity. However, the same could be said for quantitative research in which an experienced researcher would be able to identify potential confounding variables in an experimental design sooner than a less experienced researcher. Strauss & Corbin (1990) argue that a study's reliability (and some aspects of its validity) relies on the researcher's own theoretical sensitivity (Glaser, 1976).

The validity of qualitative research has not, in the past, been under serious scrutiny, since many studies do not aim to control the situations under review, but merely to capture and analyse them. Many qualitative approaches, however, are limited in their ability to produce a valid framework, which can propose implications and possible constructive interventions within a chosen field. This is often because the research only aims to describe, rather than produce a theory pertaining to, a phenomenon. Within the field of HCI it is vital, as previously stated, to make HCI knowledge accessible and applicable to designers. This requires a detailed model of relevant issues that not only describes central relationships within a phenomenon but also theoretically informed interpretations which produce complex dominant theories and principles.

Ultimately, the debate should be concerned with whether differing methods are suitable and the appropriate way to apply these approaches. Latour (1987) argues that there is basically little difference between the two paradigms as both endeavour to arrange and rearrange the intricacies of raw data. Bryman (1988) on the other hand suggests that the distinction between these two approaches is purely technical, whereby the choice between them relies on their suitability in answering particular research questions. It is suggested that a valuable approach towards strengthening the quality of research is to use a principled combination of methods (Strauss et al., 1964; Henwood & Pidgeon, 1992). It should be acknowledged by advocates of qualitative approaches that there is a lot to be learned from the quantitative paradigm just as there are lots of critical issues addressed by the qualitative approach. This therefore highlights the value of a methodology, such as Grounded Theory, that seeks to and can encompass both paradigms.

Grounded Theory model building

This section partially supports the methodological issues:

Phenomena complexity (Sub-section 10.2.3)

Structured/focused approach & Integrating mixed data (Sub-section 10.2.4)

4.3 RESEARCH METHODOLOGY: DATA COLLECTION TECHNIQUES

A Grounded Theory method was used to guide all of the study data collection techniques. This meant that the research questions were developed with the flexibility and freedom to explore the phenomena in depth. Grounded Theory data analysis also allowed for both qualitative and quantitative data sources to feed into the privacy model. A triangulation of results was used to increase their validity, as any limitations by a specific methodology or study situation would not confound the overall privacy model.

4.3.1 Focus groups

Lunt and Livingstone (1996) argue that experimentalism is too reductionistic, in its approach to data collection, to capture users' perceptions accurately because its techniques are manipulative. Focus groups, however, provide a flexible and adaptive approach to individual situations and contexts, thus ensuring a valid representation of sensitive and *Personal Information*, such as privacy factors. This methodology provides a social occasion that allows for public opinion to develop through debate as in real world situations (Lunt & Livingstone, 1996).

Focus groups consist of 3 - 7 people and aim to present as genuine and relaxed a setting as possible for naturalistic responses. The validity of the focus group relies on careful group selection (sampling). Using naturally occurring homogenous groups can aid in the production of natural conversations. However, these groups may be more eager to impress one another and be biased in their responses and should be counterbalanced with a comparative focus group. A moderator presents the focus of the discussion and helps to draw out opposing arguments without appearing judgmental of the participants' opinions. It is a difficult job for a moderator to keep the group focused yet not led by their questions or dominant group personalities.

4.3.2 In-depth interviews

Interviews provide a flexible and adaptive approach to individual situations and contexts which increases the technique's validity as a form of assessment. This flexibility provides richer and fuller information which is less likely to be biased by the researcher's own pre-conceived ideas than quantitative methods. The interviewee can feel more relaxed and less assessed as part of this procedure which increases the degree and accuracy of sensitive, *Personal Information* obtained for assessment purposes. Semi-structured elements used within the interview procedure can increase the reliability of the data obtained and allow for quicker and easier analysis. (Cooligan, 1990)

Previous background research (such as a pilot study) is essential to establish key issues and to improve interview techniques. The structure (focus) of the interview should be established before the interview

but should always be flexible so that key issues not identified before the interview emerge naturally through the discussion.

Putting participants at ease is a vital part of the interview procedure. Initial introductions are made, then permission for recording the session obtained and assurances provided for the anonymity of information taken and sensitivity with its later usage. The general background to the study should then be provided without too much detail to bias participants' responses. There are now four stages to the in-depth interview. The 1st stage will be used to obtain the respondent's background details e.g. experience with equipment, experience in general. Next some general relevant questions are asked to let the participant *let off steam* with reference to any pet hates they may have. In the 3rd stage any issues that have not already been discussed are introduced. Any unclear issues are probed for detail and further definition. This stage could require further scenario prompting - although these should be used sparingly and with great caution so as not to bias the participant. Finally there should always be a rounding off of the session with a summing up of all the issues - so that the participant believes they have presented all the information they wanted to. There should also be a reaffirmation that the information will be dealt with in the strictest confidence. A short de-briefing session may also be required to present in more detail what the research will be used for and what the aim of the research is.

4.3.3 Questionnaires

Questionnaires are effective for gathering a large amount of data in a short timeframe. There are two types of question structure (Preece et al., 1994):

- Open-ended questions allow respondents the freedom to provide their own answers. These responses provide a rich source of data that is difficult to analyse.
- Closed questions restrict the respondent's answers to a selection of alternative replies. Quantifiable scales of responses make the data easier to analyse (checklists, multi-point, Likert scale and semantic differential scale).

Again sampling in questionnaire studies is very important. It has been argued that psychological research is overly reliant on data from student populations thus biasing the results obtained. Male participants are also used more often than are females as research participants (Rohrbaugh, 1979). Questionnaire wording also plays a vital part in the biases of responses. Even very minor changes in the wording of a question can alter people's responses. For example, Loftus (1975) found that questionnaire responses varied significantly depending on the wording of the question. Ultimately to increase the validity of questionnaire results it is useful to cross-reference (triangulate¹⁵) them with other data sources.

Grounded Theory model building

This section partially supports the model method issues:
Integrating mixed data (Sub-section 10.2.4)

¹⁵ Triangulation means to compare two different views of the same things e.g. interview with observation data

4.4 CHAPTER SUMMARY

This Chapter highlights how general knowledge (see Chapter 2) and HCI knowledge (see Chapter 3) can be input into a HCI substantive and methodological knowledge base and why this should be attempted (see Section 4.1). To identify an appropriate thesis approach an evaluation of the advantages and disadvantages of the three main HCI approaches (Scientific, Craft-based and Engineering) is made (see Sub-section 4.1.1). A Grounded Theory approach has been identified to be appropriate for this thesis because it systematically builds theory based upon current and previous quantitative and qualitative research for complex phenomena with little previous research (see Section 4.2). Focus groups, in-depth interviews and questionnaires are argued as methods that will provide useful qualitative and quantitative data for this thesis (see Section 4.3).

A Grounded Theory summary of this chapter is presented in Table 4.2. This representation shows where the methodological gaps are currently in privacy research approaches, how this chapter contributes to the thesis model building and how the following Chapter will use this Chapter to develop the model.

Methodological issues	Chapters 2 & 3 methodological gaps	Chapter 4 contributions	Chapter 5 – 7 Model development
Phenomena complexity	Previous approaches could not deal adequately with the phenomena's complexity	Grounded Theory can deal with complex phenomena (see sub-sections 4.1.2, 4.2.1, 4.2.2, 4.2.3)	There is little previous Grounded Theory research within the domain of HCI upon which to build this research. This thesis research, therefore, seeks to advance empirically based HCI privacy research within multimedia communications with results that can be generalised across applications. Also see 10.2 for review of methodological contributions
Theory building	Previous approaches have not systematically built comprehensive privacy theories based on previous and current research	Grounded Theory is designed primarily as a theory building method (see sub-sections 4.1.2, 4.2.2)	
Structured / focused approach	Previous approaches have not provided applicable design recommendations that can be generalised to other applications and environments	Grounded Theory provides a focused, structured approach to research (see sub-sections 4.1.2, 4.2.1, 4.2.3)	
Integrating mixed data	Previous approaches have not provided a method for a principled mixture of both qualitative and quantitative data	Qualitative or quantitative data can be used by the analysis which does not require a prior hypothesis for focusing (see sub-sections 4.1.2, 4.2.1, 4.2.2, 4.2.3, 4.3)	

Table 4.2: Grounded Theory summary of methodological limitations and this chapters contributions

Chapter 5: Initial studies – Identifying the privacy factors

Most organisations develop privacy policies in retrospect -after an external threat to the company has been identified (Smith, 1993). This leaves most organisations and systems with privacy policies that have been superseded by changes in the organisation’s activities or the surrounding environment. Due to a lack of clearly defined factors which impact upon users’ perception of privacy and boundaries, few organisations have realised that the use of computer supported collaborative work (CSCW) systems may generate sensitive data, and that use of that data may constitute an invasion of users’ privacy. Therefore, few organisations have devised measures to safeguard such data, and thus users’ privacy.

The initial studies detailed in this Chapter aided the research both substantively and methodologically (Table 5.1).

	Contributions	
<i>Substantive input</i>	An empirical review of users’ security perceptions and attitudes to establish a context for the security paradigms’ approach to privacy and users’ perceptions (see Section 2.4)	Identification of the relevant privacy factors in the <i>privacy model</i> being developed
<i>Methodological input</i>	Development of methodologies for analysing users’ perceptions which are sensitive in nature i.e. privacy.	Development of Grounded Theory as an HCI methodology

Table 5.1: Contributions of initial studies to HCI knowledge base

The first study in this Chapter (see Section 5.1) aided in developing a background understanding of the security paradigms’ approach to privacy and users’ perceptions of security within organisations. This study also identified user security practices, behaviours and perceptions of *Information Sensitivity* (one of the three main privacy factors identified). The second (see Section 5.2) and third (see Section 5.3) studies identified and verified the three main privacy factors (*Information Sensitivity, Information Receivers and Information Usage*) in the *privacy model* for novice subjects in different environments for similar tasks. The studies also identified sub-factors and determined interactions between these factors and sub-factors causing privacy trade-offs for the task of information exchange within the domain of videoconferencing (see Section 5.2) and non-immersive virtual reality (see Section 5.3).

5.1 STUDY 1: SECURITY AND INFORMATION PERCEPTIONS

Building on from previous research into passwords (Adams, 1996), which establishes a context for the security paradigms' approach to privacy and users' perceptions, a further in-depth study was conducted using Grounded Theory. This research was used to identify user security practices and behaviours and perceptions of *Information Sensitivity* with relevant privacy implications highlighted.

5.1.1 Method

Semi-structured in-depth interviews, lasting approx. 30 minutes, were used to identify security and information perceptions with regard to password authentication systems. Interviews were conducted with 15 users from Organization A (a technically biased organization) and 15 users from Organization B (a company in the construction sector). Participants from Organization A were technically adept and used computer technology frequently for their work. Participants from Organization B were less experienced with technology and used it sporadically. Interview questions covered general security, systems and organizational issues as well as questions, not relevant to this research, about specific password generation and recall. The interview format allowed participants to introduce relevant new issues to the discussion. Grounded Theory methods (see Chapter 4) were used to analyse the interview data and identify perceptions specific and non-specific to the two comparative organizations. Two major factors influencing security perceptions were identified:

- 1) users' perceptions of organisational security and its compatibility with work practices;
- 2) users' perceptions of *Information Sensitivity*.

5.1.2 Results: security awareness

The study clearly showed that users are not sufficiently informed about security issues by the organization thus causing them to construct their own model of possible *security threats* and the *importance of security* which are often wildly inaccurate. Users tend to be guided by what they actually see - or do not. As one manager stated:

"I don't think that hacking is a problem - I've had no visibility of hacking that may go on. None at all."

Another employee observed that:

"... security problems are more by word of mouth ..."

5.1.3 Results: Information Sensitivity

The study identified the concept of *Information Sensitivity*: users rated certain types of data as sensitive or private; in turn, this perception determined the amount of effort they were prepared to expend on protecting that data. Discussions of privacy often ignore that the same data may be rated – and therefore treated - differently by different users. Without any feedback from the organization, users rated *confidential information* about individuals (personnel files, email) as sensitive; but commercially sensitive information (such as customer databases and financial data) was often seen as less sensitive. Some users stated that they appreciated the printed document classifications (e.g. *Confidential, Not for Circulation*), indicating their need for *Information Sensitivity* guidance and rules for levels of protection in on-line documentation. A common misconception by the security approach to privacy is that users make a simple binary private or not private distinction (see Sub-section 2.2.2), whereas these results highlighted that users see *Information Sensitivity* as a dimension with degrees of *Information Sensitivity*.

Grounded Theory model building

This section partially supports the model factor:

Information Sensitivity: Judgement (Sub-section 8.3.2.1)

5.1.4 Results: Using Grounded Theory to identify privacy problems

The analysis provided a step-by-step account of user authentication usage problems and possible intervention points. Key privacy issues identified through research at Organisation A were substantiated and expanded upon by the research in Organisation B. A detailed account of memo notes and analysis procedure can be found in Appendix 1. This study identified two major *benefits* in using Grounded Theory as an HCI methodology in identifying privacy issues

- i. Because of Grounded Theories conceptual depth (a hierarchical analysis with cross-links) and no pre-defined theory to restrict research testing the data could be tested and re-tested to identify the source of initial contradictions in the data. This means that whole data sources are not disregarded because of confounding contradictions (see Sub-section 5.1.4.1).
- ii. Because Grounded Theory relies on interview questions that are flexible this allowed different sample perceptions to be analysed with regard to issues which did not emerge until the data was analysed. This means that valid and complex relationships can be identified in shorter timeframes (see Sub-section 5.1.4.2).

5.1.4.1 Security perceptions: solving apparent contradictions

Several of the interviews showed that users stated one perception of their behaviour and then later the opposite. Such *contradictions* made it hard to establish relationships between factors which influence

user behaviour. Contradictory statements could be caused by users being unsure of their own descriptions, or discussing complex issues which involve several factors. The application of Grounded Theory techniques for analysing the free-format statements in the data identified the latter as the case. An example of an apparent contradiction is shown in Table 5.2 & Diagram 5.1.

Perceptual type	Security perceptions	Resultant security behaviours
A	If users perceive the organisation's general security level as low (decreased), this decreases their perception of how sensitive the data protected is.	The result is a decrease in secure work procedures. ("Well, if the information isn't important, why make a big fuss about keeping it secure?")
B	If users perceive the organisation's general security level as high (increased) this then decreases their overall perception of threats to the data.	The result is a decrease in secure work procedures ("Well, security for getting into the site is so tight, and there's nobody who'd want the information why should I go out of my way to keep it secure.")

Table 5.2: User behaviours produced by perceptions of security levels

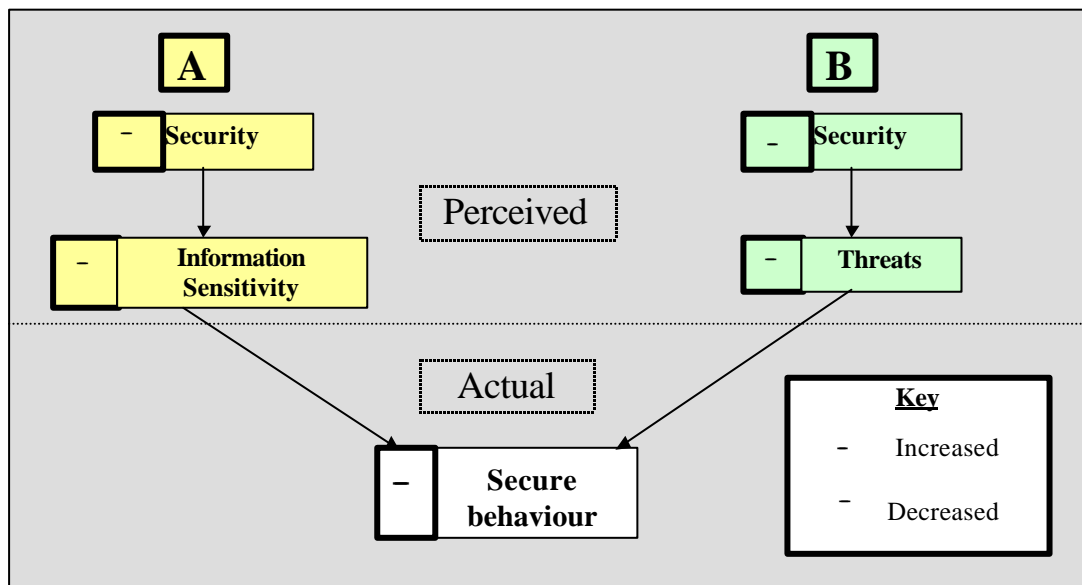


Diagram 5.1: User behaviours produced by perceptions of security levels

Grounded Theory model building
 This section partially supports the model factor:
Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

5.1.4.2 The importance of work practices from differing perspectives

The analysis revealed the importance of compatibility between work practices and security procedures. Organisations A and B forced users to undertake security procedures that in different ways users perceived to be incompatible with the nature of their work and the information involved in it (see Diagram 5.2). Although both organisations had different work practices and data types, users from both organisations rejected the incompatible security mechanisms.

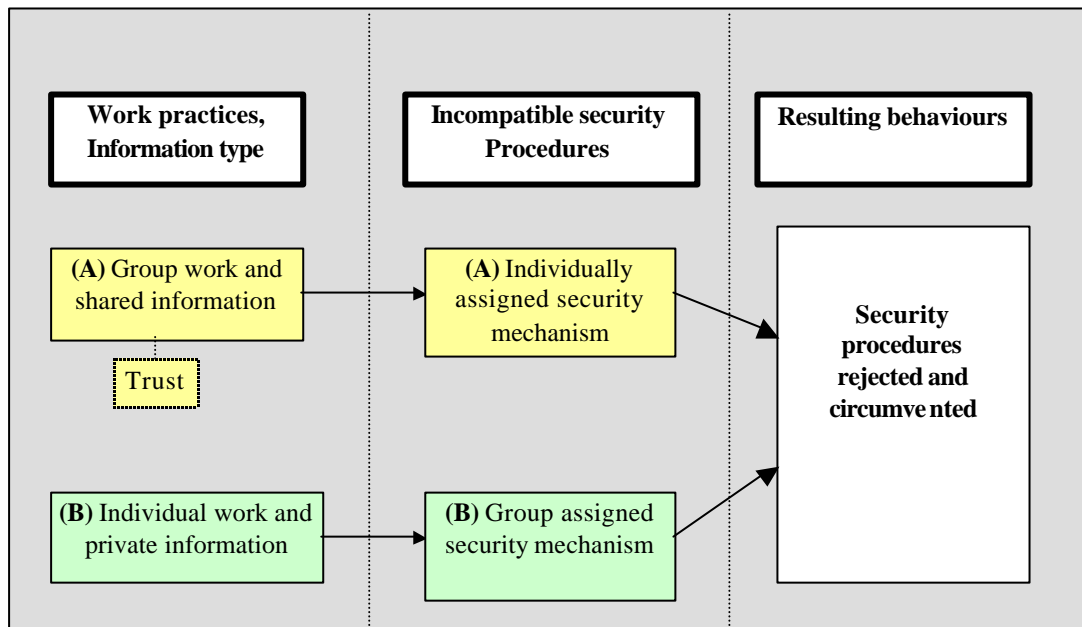


Diagram 5.2: Users' perceptions of work practices and system procedures

5.2 STUDY 2: DESKTOP VIDEOCONFERENCING

Results from study 1 (see Section 5.1) and an analysis of the literature review (see Chapters 2 and 3) were used to identify a focus for this study. Study 2 was primarily used to identify the *privacy model* factors and potential environment specific and non-specific interactions between sub-factors.

5.2.1 Method

The desktop VC system used combined a number of multicast conferencing tools (Kirstein et al., 1995):

- rat for audio;
- vic for video¹⁶;
- and a shared whiteboard, wb.

¹⁶ Multicast audio and video are sent in separate streams. Synchronization requires at least 8 frames of video per second. Decoding this from 5-6 participants per group was deemed too high. In previous studies, lack of synchronization was not detrimental to learning, so course organizers used 5-6 frames of unsynchronized video.

The user group consisted of 35 undergraduate students in Information Management at UCL. All users encountered desktop videoconferencing for the first time at the beginning of this project. The VC system was used for information exchange tasks (tutorials) which had previously been completed face-to-face. The students completed an introductory session in videoconferencing at the beginning of the course. Each student sat at their own workstation during the 8 weekly sessions, discussing a set of questions on a computer-networking course (the course material itself was provided on a CD-ROM). The tutor, who was located at a different university, would join those sessions after 30 minutes, and work with students for another 30 minutes, checking the answers students had come up with and probing the depth of their understanding.

5.2.1.1 Focus groups

Users discussed their experiences with the system in focus groups, which provided a flexible and adaptive approach to individual situations and contexts, thus ensuring a valid representation of sensitive and *Personal Information*, such as privacy factors (Lunt & Livingstone, 1996).

Although users were free to raise any relevant issues they wanted to, the main issues debated (introduced by the moderator) were:

- Key privacy issues of *Information Receiver, sensitivity and usage*.
- Task (educational information exchange) issues.
- Student-student or student-supervisor interactions.
- System design issues.
- Comparisons between system-mediated and face-to-face interactions.

All participants agreed to the session being audiotaped and were assured that the data would be stored in an anonymous form and treated with the strictest confidence. Users were also informed that they could leave if they felt the session became too uncomfortable and that they would be debriefed at the end of the focus group.

5.2.1.2 Longitudinal study

Longitudinal studies can identify issues affected by time factors and provide rich, genuine information that has a high validity. Focus groups were, therefore, conducted both at the beginning and end of the students' course in weeks 4 and 8. It was hoped that this would obtain initial privacy perceptions to contrast with those obtained later. The focus group sessions (in groups of 6 -10) were kept the same throughout the course. Grounded Theory uses a continual comparison technique across all the data collected and can therefore be used effectively to identify similarities and differences across focus groups.

5.2.2 Results: Consistent perceptions

The longitudinal nature of this study meant that perceptions which persisted, over the eight-week period, could be identified.

5.2.2.1 Information Sensitivity

Two important factors relating to *Information Sensitivity* within multimedia communications were identified. Firstly there are two different levels at which information can be perceived with regard to its sensitivity.

- *Primary information* relates to the topic of discussion.
- *Secondary information* relays other interpretative social-psychological characteristics about the user.

Primary information may greatly affect the perceived sensitivity of *secondary information* or vice versa. As *secondary information* often relates to information that defines the user in a particular way this can retain a higher sensitivity than *primary information*. Often, privacy risks associated with *primary information* are noted and assessed by users and organisations but the *secondary information* (a source of many user assumptions and misconceptions) is overlooked.

Secondly the media of transmission affects the degree of *secondary information* released and thus the sensitivity of the information interpreted. With the use of multimedia there is a relative increase in *secondary information*

- Text (textual cues) - the presentation of the data, type of language used.
- Audio (verbal cues) - tone of voice, accent, dialect, gaps in conversation.
- Video (visual cues) - dress & appearance, mannerisms.

Although users' perception of *Information Sensitivity* is vital in establishing privacy risks the results identified that if information is perceived as sensitive an assessment of the *Information Receiver* (IR) becomes paramount before data is released. For example, students noted that if multimedia information presented them in an embarrassing way (e.g. they answered a question wrong so they perceived that they looked stupid) they wanted to know who was viewing the information and why.

Grounded Theory model building

This section partially supports the model factor:

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

Information Sensitivity: Trade-off's (Sub-section 8.3.2.4)

Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

5.2.2.2 Information receiver

Privacy risks associated with the *Information Receiver*, such as vulnerability and trust, can restrict self-expression and personal development. This highlights the issue of whether it is what is known about a person that is invasive or who knows it. A range of issues will influence the users' assessment of the *Information Receiver*(IR):

- the users' experience of the *Information Receiver*;
- a range of social, organisational and cultural norms;
- the particular interaction setting (environment, task, system).

This study highlighted that when users deem information to be potentially sensitive there is a need for greater benefits from disclosure if the *Information Receiver*(IR) is personally known.

A sub-factor influencing users' perception of the *Information Receiver* is *Relationship* (Close, distant, unknown). It could be argued that because highly sensitive information is more representative of a person, there is a higher risk of embarrassment with an *Information Receiver* who has a close relationship with the user, than with a complete stranger.

“If I know them and they know me personally then I don't like it”.

We may not mind how Joe Bloggs (a stranger, whom we are never going to meet) views us, our beliefs and our attitudes, but if he is the son of our next door neighbour the personal risks involved increase ten fold (or more).

The results also identified the importance of the *Role* of the *Information Receiver* with regard to the information and its usage.

“I don't mind tutors because somehow I feel that tutors have to act right”

Someone highly trusted may be able to view highly sensitive information but only if they are deemed to have an appropriate role in the information. Of key importance with both of these issues was the feedback that users received with reference to who was receiving this information both currently and at a later date.

Grounded Theory model building

This section partially supports the model factor:

Information Receiver: Trust (Sub-section 8.3.3.1)

Information Receiver: Relationships (Sub-section 8.3.3.2)

Information Receiver: Trade-off's – trust (Sub-section 8.3.3.3)

Information Receiver: Trade-off's – roles (Sub-section 8.3.3.4)

Information Usage (IU): Current IU – task (Sub-section 8.3.4.1)

Context: Technology – environments (Sub-section 8.3.5.1)

Context: Social groupings – social groups (Sub-section 8.3.5.2)

Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

Context: National and international – cultural norms (Sub-section 8.3.5.8)

5.2.2.3 Context (Interface issues)

The study identified the importance of the technology, which mediates the interaction and specifically the users' *Presence* within the environment (also identified within the Virtual Reality study – Sub-section 5.3.2.2). Within the study the lack of synchronization between audio and video resulted in users' feeling disembodied from the context.

“I suppose it's easier to forget who's listening in, that's the point, you know, because you have to actually physically look at people on the screen.”

Although this factor increased the users' perceived distance from the group and presence in the context it had a positive effect on users' concentration.

“That's like distracters. 'Cause you've got no one next to you to sort of pull you off of what you're supposed to be doing.”

Users felt less intimidated by others' presence or the likelihood of making embarrassing mistakes and more able to express themselves freely which resulted in an adjusted behaviour of disclosing more information. Users also noted that they felt a greater need to actively *participate* in the interaction, as their mere virtual presence was not enough to warrant social approval.

Grounded Theory model building

This section partially supports the model factor:

Context: Technology – environments (Sub-section 8.3.5.1)

Context: Technology – interface issues (Sub-section 8.3.5.2)

Context: Technology – presence (Sub-section 8.3.5.3)

Context: Social groupings – social groups (Sub-section 8.3.5.2)

Context: Social groupings – social group outsiders (Sub-section 8.3.5.5)

5.2.3 Results: Changing perceptions

As this was a longitudinal study it enabled some comparisons between initial and later perceptions to be conducted so that changes in perceptions could be identified.

5.2.3.1 Information Sensitivity

As users' understanding of the technology's capabilities increased they questioned how it could affect the data transmitted and interpreted by those receiving it. Users' started to question how lighting effected the image received, and what effect delay in data transmissions had on video quality received by the recipient (were they being made to look stupid by the image). For example, a system that allows the *Information Receiver* to freeze frames, so that they appear to be avidly viewing the screen but instead have actually gone to make themselves a cup of tea, could produce an inaccurate appraisal of their attention within the interaction. This, in turn, produces potential privacy mismatches (if, for example, someone else views the meeting from the *Information Receiver's* seat) between the real and what the user perceives as the *Information Receiver*.

It is important to note here that within most multimedia interactions (with a system or another user) a user is both an *information broadcaster* and *receiver*. This user distinction is important because it is as a *broadcaster* that the user takes *privacy risks* and as a *receiver* that the user receives *benefits* and privacy norms are enacted. Virtual situations can clearly divide these roles and increase the importance of appropriate feedback and control. Within many videoconferencing applications the user can zoom in on images without the *Information Broadcaster* realising it, whereas in the real world it would be obvious if someone was staring at you and getting closer.

Another changing perception identified affecting users' privacy perceptions is that of *Information Sensitivity* relating to its primary and secondary levels of content. Technical details of a process discussed within an email conversation would be *primary information*. As already noted, the *privacy risks* associated with this low sensitivity *primary information* are low

"It's not something major somebody tapping in - because it's about course work".

However, if the user realised at a later date that the information released was highly sensitive at a secondary level their perceptions of privacy risks would be greatly increased. A user relaying obviously incorrect technical details would portray his lack of knowledge and understanding of the data and thus turn low sensitivity *primary information* into highly sensitive *secondary level information*

"...if they were looking at our reactions then I wouldn't mind but if they were making comments about what we were saying on the course work - which is really crap, we know nothing - then...."

Mismatches between the perceived and actual privacy risks can be reinforced by system design (not being able to see what data is being disclosed) policies,

"But I think there's so much material and it takes so long to go through it all it becomes sort of impersonal by the end of it. I mean what do you guys do with it (worried note in his voice)."

and personal biases (nobody would want to know about me I'm not important enough).

Grounded Theory model building

This section partially supports the model factor:

User factor: user distinction (Sub-section 8.3.1.2)

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

Information Sensitivity: Trade-off's (Sub-section 8.3.2.4)

Context: Technology – interface issues (Sub-section 8.3.5.2)

Privacy invasion cycle (Section 8.1) Grounded Theory analysis identified the *privacy model* as the core category and the *privacy invasion cycle* as its' story: a descriptive narrative of how the privacy model factors relate to privacy invasion. This study highlighted the importance users' realisation or *awareness* that their privacy perceptions were inaccurate.

5.2.3.2 Information Usage

The use to which data is ultimately put may affect users' concerns about information technology. Strong links were identified between the later usage of information and its perceived sensitivity. However, the key issue surfacing from this study is that the mismatch between the perceived and

realised actual data usage produces privacy problems despite the sensitivity of the information. This study highlighted that there were two important elements in *Information Usage*, with reference to users' privacy; *Recording Awareness* and *Context of usage*.

If users assume that data is not recorded, their perceptions of privacy risks decrease (thus increasing *trust* in the system and *Information Receiver*) which in turn leads to an increase in information disclosure. If, however, the data is actually recorded, perceptions of privacy risks increase;

“..... I'd be personally quite worried if somebody told me at the end of the session that, right you've been listened to. I mean I'd go back and say 'did I say something I shouldn't have said.' Especially if you know the person who listens to it. The next time you see them you feel a bit awkward - did they remember what I said?”

What is vital here is the *realisation* of a mismatch producing a decreased *trust* in the *Information Receiver* or System.

The findings demonstrate that when low sensitivity data is taken out of context it can sometimes become highly sensitive, personally representational information showing the user in a bad light. The longitudinal results identified the important concept of data *context* in its usage as information. Users' perceptions of privacy risks increased greatly when they realised that data assumed to be used in context, could actually be used *out of context*

“*Out of context and then it would be a big problem.*”

Grounded Theory model building

This section partially supports the model factor:

Information Usage (IU): Later IU – recording awareness (Sub-section 8.3.4.2)

Information Usage (IU): Later IU – context (Sub-section 8.3.4.4)

Privacy invasion cycle (Section 8.1): realisation or awareness that users' privacy perceptions are inaccurate.

5.3 STUDY 3: VIRTUAL REALITY

The interaction environment can allow for different degrees of anonymity, which in turn may affect users' perception of privacy. The task and participants' experiences may also interact with the media and make the technology-mediated situation unacceptable. This study aimed to compare a virtual reality environment with the videoconferencing study for *privacy model* factors.

5.3.1 Method

The prototype Virtual Reality (VR) system was introduced to a group of 9 Ph.D. students at UK universities, sponsored by British Telecom. All the participants' encountered VR for the first time during this study. The VR system reviewed was at the prototype stage and was being developed by researchers at British Telecom. The VR system was used for information exchange tasks (student

networking and supervisor contact) which had previously been completed face-to-face. The system was designed to help users, who do not usually interact, to collaborate with each other.

The VR prototype system was initially demonstrated (assisting *envisionment*, a central process to participatory design) to the students and followed by a question-and-answer session. Finally, students participated in two-hour focus groups, discussing collaborative and privacy issues of the system.

The prototype system was demonstrated with the following facilities: audio, animated avatars, whiteboard tools, links to WWW pages, notice boards and videoconferencing. Students could conduct presentations of their research and produce on-line references for those interested.

5.3.1.1 Focus groups

Participants assessed the application for the task of discussing and debating their research with peers and supervisors who would also provide advice and assess their research. Participants reviewed the system for peer and non-peer information sharing and educational dialogue. Differences between student-student and student-supervisor interaction were investigated to ascertain the importance of social roles on autonomy and degrees of privacy. The key privacy issues for this environment and comparisons between system-mediated and face-to-face interactions were identified.

The moderator guided the discussion by probing for insights, without confounding results by prompting with leading, restrictive questions. All participants agreed to audio taping of the session and were assured that the data would be stored in an anonymous form and treated with the strictest confidence. Users were also informed that they could leave if the session became too uncomfortable and that they would be debriefed at the end of the focus group.

5.3.2 Results

The results from this study were used to corroborate factors identified in studies 1 & 2 whilst identifying issues specific to this environment.

5.3.2.1 Information sensitivity

This study corroborated study 2's findings that users can interpret the same data in different ways. A misinterpretation of *Information Sensitivity* can be due to primary and secondary levels of the information (see Sub-sections 5.2.2.1 & 5.2.3.1). Initially the *primary information* (topic of discussion) is captured and assessed by the user for its risk value. However, the interpretative social-psychological qualities in the *information's secondary level* are overlooked in this assessment. The invasiveness of this oversight may be due to how much it defines the social-psychological characteristics of the user and thus personally represents them in a particular way. Similarly, someone could view their address as being impersonal representational information but later realise that it could be potentially invasive by reflecting their earning abilities if they were grouped within a poor economic area. The key factor in this interaction is the realisation that a misjudgement has been made. The

user's assessment of the risk involved in the situation is thus inaccurate and their control of the potentially invasive material, which Bellotti (1997) highlighted as vital, is lost.

Grounded Theory model building

This section partially supports the model factor:

Information Sensitivity: Judgement (Sub-section 8.3.2.1)

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

Privacy invasion cycle (Section 8.1): realisation or *awareness* that their privacy perceptions were inaccurate.

5.3.2.2 Information receiver

The issue of the *Information Receiver's* relationship with the user did not surface within this study. This is probably due to the fact that all of the participants were strangers and evaluated the system as a collaboration tool between students who do not know each other.

However, the study's results did identify the importance of the *Information Receiver's role* in the information and its usage. Someone highly trusted may be able to view highly sensitive information but only if they are deemed to have an appropriate role in the information. Of key importance is feedback to users on who is receiving this data both currently and at a later date.

Grounded Theory model building

This section partially supports the model factor:

Information Receiver: Trust (Sub-section 8.3.3.1)

Information Receiver: Trade-off's - roles (Sub-section 8.3.3.4)

5.3.2.3 Information Usage

Finally the results corroborated the importance of the third factor in the framework - *Information Usage*. Strong links were identified between later data usage and its perceived sensitivity. Users were ardent in their need for prior knowledge of any data usage, even if they later decided they had no problems with its usage because of its low sensitivity. The determining issue seems to be that there is a need for prior knowledge to make appropriate risk assessments. This finding again corroborates Bellotti's (1997) arguments on the importance of user control and feedback. Users' perception of control was found to be essential in building *trust* relationships for effective social interaction. A user's ignorance of a session being recorded or of *Information Usage* may cause discomfort when later realized because of imagined embarrassing scenarios that may be no less likely if the user had known of the recording. The important difference is the users' perception that they would have more control of the situation if they had known.

The study again highlighted, as previously suggested by Dix (1990), the issue of keeping data in context (see Sub-section 5.2.3.2). It was noted, though, that this was strongly connected to *trust* in the

Information Receiver and the collaborative sense of sharing. However, once this *trust* had been abused the participants suggested that they would not be able to reinstate it through this system.

Grounded Theory model building

This section partially supports the model factor:

Information Receiver: Trust (Sub-section 8.3.3.1)

Information Receiver: Trade-off's – roles (Sub-section 8.3.3.4)

Information Receiver: Trade-off's group membership (Sub-section 8.3.3.5)

Information Usage (IU): Later IU – recording awareness (Sub-section 8.3.4.2)

5.3.2.4 Context

The study results again identified the importance of the interaction environment with regard to users' *presence* within the environment (see Sub-section 5.2.2.3). This factor increased users' perceived anonymity that in turn decreased perceived *privacy risks*. Perceived anonymity was found to have positive effects upon users' task focus and freedom of expression (see Sub-section 5.2.2.3).

“In certain environments you're relatively anonymous so you can give your real opinions rather than saying what you think you ought to say.”

However, contrary to videoconferencing environments, users felt increased implicit presence in the environment by empathising with their avatar. The result of these findings is that although users felt the anonymity gave them increased freedom of expression, this was counter-acted by implicit social norm pressure (e.g. embarrassment when walking up to a group of avatars talking – 'should I interrupt?').

Although the VR users communicated using both audio and images, they still perceived an increase in anonymity levels because of the artificiality of the environment (using avatars) in which interactions took place. This perceived anonymity increased users' perception of *safety* (from privacy invasion) within and *control* of the environments. However, results also highlighted that if the user was actually identifiable (e.g. via their voice, name) and the system had failed to clearly illustrate this, a privacy mismatch would occur when the users realised this fact.

Finally, it was noted that the environments' tools sometimes made information exchange easier than in face to face situations: no social pressures restricting access to the whiteboard and easier access to extensive on-line information (WWW links).

Grounded Theory model building

This section partially supports the model factor:

Information Usage (IU): Current IU – task (Sub-section 8.3.4.1)

Context: Technology – environments (Sub-section 8.3.5.1)

Context: Technology – interface issues (Sub-section 8.3.5.2)

Context: Technology – presence (Sub-section 8.3.5.3)

Context: Social groupings – social groups (Sub-section 8.3.5.2)

Privacy invasion cycle (Section 8.1): realisation or *awareness* that their privacy perceptions were inaccurate.

5.4 CHAPTER SUMMARY

A lack of communication between security departments and users was identified as due to the security paradigms' *need-to-know* principle. Users are considered by security departments as *inherently unsafe* whilst inadequate user security knowledge produces their insecure behaviors. Users guide their security perceptions by their own judgments of information's sensitivity or visible threats (see Section 5.1). Studies 2 and 3 further identified that within multimedia communications, there are two levels of information relayed: *Primary* information relating to the topic of discussion, whilst *secondary* information relays other interpretative social-psychological characteristics about the user via visual, auditory or textural media (See Sub-sections 5.2.2.1, 5.2.3.1, 5.3.2.1).

Close relationships between the user and *Information Receiver* were identified in study 2 as requiring higher *benefits* to trade-off against potential *privacy risks* before data is released. Studies 2 and 3 also noted that the *Information Receivers'* role in the data usage will affect perceived sensitivity levels of the information and potential trade-offs made by the user.

Studies 2 and 3 highlighted the importance of users' awareness of recording sessions thus allowing users to make accurate judgements of potential *privacy risks* prior to data transmission. It must not be forgotten, however, that the context in which the data is used at a later date is also an important issue.

Finally the users' perception of their presence within the context of social interaction has also been highlighted as an important factor in the perception of what data is received. Users' presumed anonymity yet empathy with avatars could cause privacy mismatches. Democratic use of environmental tools increased their freedom to express themselves and be creative unconfined by social pressures (ridicule etc.)

A Grounded Theory summary of research from this chapter is presented in Table 5.3. This representation shows how the research presented in this chapter expands the privacy model being developed, where the gaps are currently in the model and how the following chapter will expand on the model.

Model Factors	Chapter 5 Privacy model contributions	Factors verified and model gaps	Chapter 6 Model development
USER FACTORS		The studies verified and expanded upon the user factors identified in previous literature. However variation in system interaction were not reviewed.	Chapter 6 will identify and expand upon previously identified privacy model factors and any trade-off's that are made with variations in users' system interaction levels and organisational trust.
<i>Mental models</i>	Sub-sections 5.2.2.3, 5.3.2.4		
<i>User distinction</i>	Sub-section 5.2.3.1		
INFORMATION SENSITIVITY (IS)		Information judgement and primary / secondary factors were verified with new trade-off's between these factors identified. The private / public divide, however, was not established.	
<i>IS Judgements</i>	Sub-sections 5.1.3, 5.3.2.1		
<i>Primary / secondary information</i>	Sub-sections 5.2.2.1, 5.2.3.1, 5.3.2.1		
<i>Trade-off's</i>	Sub-sections 5.2.2.1, 5.2.3.1	The information receiver issues of trust, relationship and trade-off's identified by previous research were verified for multimedia communications. Interactions between IR and other privacy factors have not been fully explored.	
INFORMATION RECEIVER (IR)			
<i>Trust</i>	Sub-sections 5.2.2.2, 5.3.2.2, 5.3.2.3		
<i>Relationships</i>	Sub-section 5.2.2.2		
<i>Trade-off's – trust</i>	Sub-section 5.2.2.2		
<i>Trade-off's – roles</i>	Sub-sections 5.2.2.2, 5.3.2.3		
<i>Trade-off's – group membership</i>	Sub-section 5.3.2.3	Studies 2 and 3 verified task, recording awareness and context IU factors. Repeated viewing, editing and risk/benefit trade-offs were not identified.	
INFORMATION USAGE (IU)			
<i>Current IU – task</i>	Sub-sections 5.2.2.2, 5.3.2.4		
<i>Later IU – recording awareness</i>	Sub-section 5.2.3.2, 5.3.2.3		
<i>Later IU – context</i>	Sub-section 5.2.3.2	Studies 1, 2 and 3 verified, for multimedia communications, and expanded upon all of the contextual issues highlighted in previous research with the exception of organisational trust.	
CONTEXT			
<i>Technology - environments</i>	Sub-sections 5.2.2.2, 5.2.2.3, 5.3.2.4		
<i>Technology – interface issues</i>	Sub-sections 5.2.2.3, 5.2.3.1, 5.3.2.4		
<i>Technology – presence</i>	Sub-sections 5.2.2.3, 5.3.2.4		
<i>Social groupings – social groups</i>	Sub-sections 5.2.2.2, 5.2.2.3, 5.3.2.4		
<i>Social groupings –outsiders</i>	Sub-section 5.2.2.3		
<i>Organisational culture –norms</i>	Sub-sections 5.1.4, 5.2.2.1, 5.2.2.2		
<i>Nat/international – cultural norms</i>	Sub-section 5.2.2.2	Cycle awareness factors identified	
PRIVACY INVASION CYCLE	Sub-sections 5.2.3.1, 5.2.3.2, 5.3.2.1, 5.3.2.4		

Table 5.3: Grounded Theory research summary for studies 1,2 and 3, model contributions and gaps

Chapter 6: Privacy threats study

The rapid advance of network and compression technology is quickly increasing the number and variety of uses for networked multimedia applications. These applications allow users to access and continuously record conferences, lectures and even to enjoy the view from someone else's office window anywhere in the world (e.g. 'Places all over the world'¹⁷). With the immense possibilities that are evident with this technology come potential *privacy risks*. This thesis seeks to identify and detail the relationship between multimedia data and privacy invasion. Whilst the initial studies identified privacy factors with multimedia data (see Chapter 5) the studies reported in this and the following Chapter seek to develop and verify the *privacy model* for different users and contexts. The study of *privacy threats* establishes users' perceptions of the *privacy risks* associated with multicast transmission of their presentations and discussion contributions on the Internet. This scenario was chosen because it represented a highly technical, trusting environment where there had been no previous backlashes to privacy invasion.

6.1 PRIVACY THREATS STUDY (study 4)

This study reviews the privacy implications of transmitting conferences via the multicast backbone (Mbone). The Internet Engineering Task Force (IETF) is an open international community concerned with technical aspects of the Internet architecture and its operation, and is open to any interested individual. The work of the IETF is done in working groups, via mailing lists and the IETF meetings three times a year. The first multicast transmission was from the IETF meeting in 1992. The original idea was to construct a semi-permanent IP multicast test bed to carry selected IETF session transmissions and support continued experimentation between meetings. Multicast of selected sessions was proposed to allow those who could not attend the IETF meetings to watch these sessions remotely and ask questions (Deering, 1989). Recording of sessions was later introduced to reduce the negative effect of global time differences. Sessions can now be watched at convenient times and days throughout the world.

6.1.1 Method

Selected IETF sessions are multicast from every meeting, using multicast tools such as *rat* (Hardman et al., 1998), *vic* (McCanne & Jacobson, 1995) and *wb* (McCanne et al., 1996) to transmit audio, video and shared whiteboard data. There are several thousand sites all over the world that have the connectivity and tools required to receive the transmissions. The fact that a session is multicast is noted on the agenda of the sessions. However, no announcement of sessions being multicast is made at the session itself, although the presence of microphones (only used for multicast purposes) and cameras could be argued to provide a clear visual clue.

6.1.1.1 Participants

Participants were conference attendees who had presented or spoken out at a session, in the previous IETF, which was transmitted over the Internet. Many of the participants had presented at several multicast IETF sessions over the past 7 years. All 24 of those interviewed had a high level of technical knowledge about networks in general. Even though the majority of participants had little experience of watching the IETF sessions remotely (because they usually attended them in person), they had viewed other events remotely using the same technology. Most of the participants had been attending the IETF since it began and had a high degree of trust in the organisation as a whole and multicast technology in particular. The participant sample¹⁸ was selected to be representative of the IETF population.

6.1.1.2 Study procedure

All participants who had presented at or contributed to a multicast session at the 41st IETF meeting in Los Angeles were contacted by email and invited to participate in an interview (lasting approx. 30 minutes) during the 42nd IETF meeting in Chicago. Participants were assured of the anonymity of their responses and the strictest confidence that would be taken with data storage and information analysis.

Those interviewed were initially asked open-ended questions about their perceptions of the IETF, multicast technology and privacy followed by specific questions on their perceptions of:

- who would be viewing the multicast sessions (*Information Receiver*);
- how sensitive was the multimedia session data transmitted (*Information Sensitivity*);
- how the recorded multicast sessions would be used and re-used (*Information Usage*).

6.1.2 Results: High-level analysis

Initial open coding of the transcripts resulted in some descriptive statistics that provide an overview of participants' perceptions (see Table 1 and Diagram 1). The descriptive statistics show the percentile of interviewees who raised a particular issue as an existing or potential threat to privacy. The majority (67%) of respondents raised issues relating to *Information Usage* as the main threat to their privacy: via the unauthorised editing, out of context, of recorded multicast data (see Diagram 6.1, Table 6.1). The presentation of such data out of context can increase the potential misinterpretation of the information. It is interesting to note that a quarter of respondents were also worried about *information usage* via editing of emotive sessions and thus misrepresenting the respondents (e.g. as irrational, over-emotional, irritating).

¹⁷ Multicast address: 224.2.172.238/51482

¹⁸ Majority male, western, high socio-economic background

The descriptive statistics identify that outsiders receiving the multimedia data is perceived by a quarter of the participants as a threat to privacy through changes in session dynamics (e.g. stifling debates, influencing debates). It is, however, important to note that the majority of respondents did not initially note that *Information Sensitivity* was a source of potential privacy invasion. Further analysis (see Sub-section 6.1.3), however, revealed that this initial perception was the result of *Information Sensitivity* misconceptions, which in turn produced unintentional invasions of privacy.

	Issue title		Summarized description	% response
Information Sensitivity	Non-Participants		Non-participants viewed (sleeping, leaving)	12.5%
	Emotive Sessions (1)		Emotional sessions being broadcast	10%
Information Receiver	Outsiders		Outsiders changing session dynamics	25%
	Remote Viewers		Misinterpreting sessions due to a lack of context	12.5%
Information Usage	Recording	Out of Context (1)	Recording and reviewing without time-reference	10 %
		Emotive sessions (2)	Emotive session recording	12.5%
	Editing	Out of context (2)	Editing	67%
		Emotive session (3)	Editing potentially misrepresenting	25%

Table 6.1: Categories of potential privacy issues

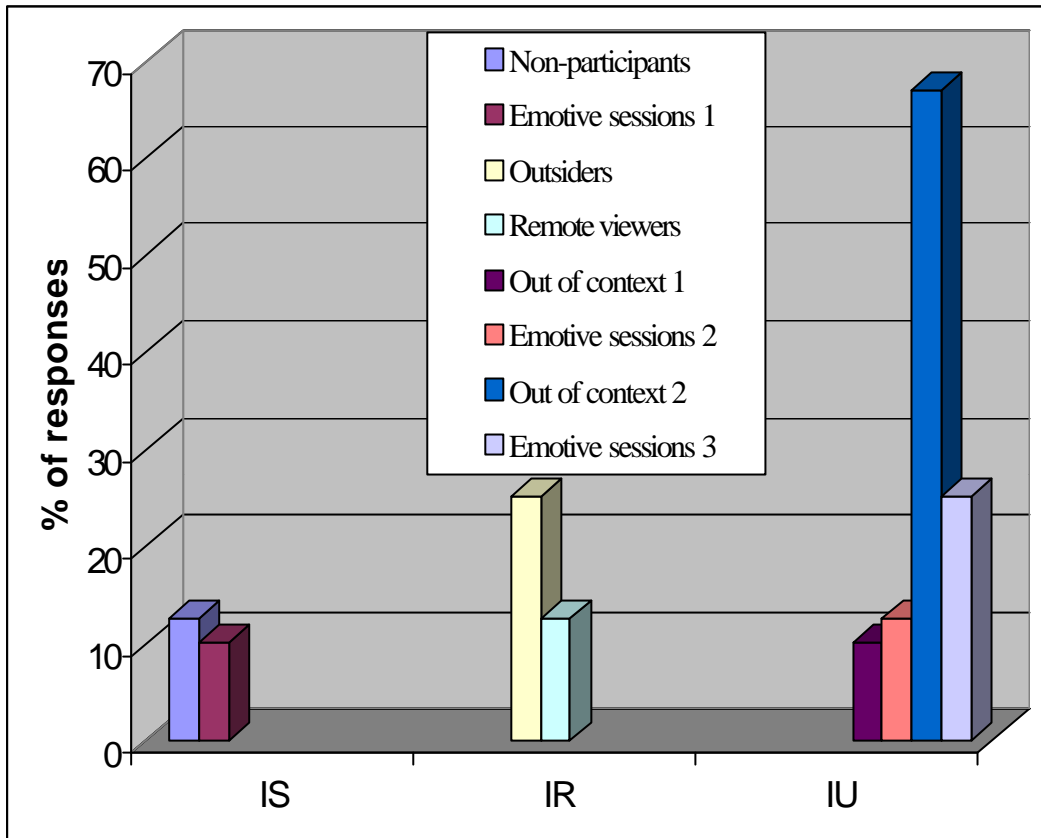


Diagram 6.1: Users' Perceived Privacy Problems

Although useful as an overview the descriptive statistics do not reflect how much of a threat any particular issue was seen to be by the participants. These results also do not reveal users' perceptual misconceptions and changes in their perceptions when factors interact. The Grounded Theory analysis of the responses revealed the relative importance of each issue. These results are described in detail for each privacy factor, and illuminated by examples of users' perceived privacy invasions.

Grounded Theory model building

This section partially supports the model factor:

Information Usage (IU): Later IU – editing (Sub-section 8.3.4.5)

Context: Social groupings – social group outsiders (Sub-section 8.3.5.5)

6.1.3 Results: detailed analysis

An overriding factor affecting users' perceptions within this study was the high degree of *trust* felt by the conference attendees in the technology (IP multicast) and the organisation (IETF) instigating the technology. With this trust-bond there is an implicit acknowledgement that the trusted party will retain their best interests and not betray that trust. Many interviewees were not aware of the privacy implications of the technology. As one interviewee noted when talking about his own privacy concerns:

“But I have no clue that that has ever happened.”

However, the results highlighted that many of the privacy invasions identified as potential *threats* had already occurred and were likely to continue if they were not addressed. Subsequent breaches in *trust* were identified as having serious consequences. Ultimately, users' *trust* and apparent lack of concern for privacy issues should not allow organisations to become complacent in privacy policy and design programs.

Grounded Theory model building

This section partially supports the model factor:

Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

Context: Organisational culture – trust (Sub-section 8.3.5.7)

6.1.3.1 Information Sensitivity

A clear finding from this study is the importance of users' *Information Sensitivity* misconceptions. The results from this study substantiated and expanded upon previous results (see Sub-section 5.2.2.1) of *primary* and *secondary information* affecting *Information Sensitivity* levels. Although participants viewed the information at its primary level others could interpret it, remotely, at its secondary level.

The majority of participants initially perceived the *risk* of having their privacy invaded, via multicast sessions, as low because of its content:

“We don't even want to listen to this – who else would?”

Yet, the multimedia data transmitted can be interpreted at more than one level. An *Information Sensitivity* issue, raised by 10% of participants, was that arguments in sessions occasionally became *emotive* (heated), and that this could be potentially embarrassing for those involved:

“Presumably that would be the type of session that you'd be more likely to say something you didn't intend to have publicly known.”

Ultimately, information at the technical (*primary*) level was perceived as having a low sensitivity yet sensitivity levels increased with debate content of the sessions become *emotive (secondary level)*

The users, however, are not the only ones who misinterpret *Information Sensitivity* levels. Many multimedia designers and initiators can make decisions based on their own inaccurate perceptions of the situation and the data's sensitivity. Study results highlighted that problems occurred when users' perceptions did not correspond with these perceptions. This perceptual conflict was identified as a major reason why unintentional invasions of privacy occurred so frequently with the IETF session data.

When conference camera operators transmitted images of attendees in sessions they were implicitly assuming that this data retained the same acceptable sensitivity as for those presenting. They may have decided, for example that as hundreds of people attend the session, some more people viewing them remotely would not be particularly more invasive. However, the attendees in the real-world situation could see who was watching them and who was not whereas, when sessions were transmitted there was no awareness of who was watching. The transmission of *non-participants'* (people who were not actively participating in a session) images was not only mentioned by 12.5% of interviewees, but was also seen to be of great importance by those who mentioned it:

“That does feel like an intrusion on your privacy, to have them video taping you when you’re just sitting off in the corner [a non-participant] - you know, having a conversation with somebody or falling asleep.”

It should be noted that this issue could relate to users’ perceived level of system interaction. Those presenting at a session felt that they understood it was being multicast and assumed that they understood the *privacy risks* involved, and could adjust their behaviour accordingly. Those that stood up, on the spur of the moment, to ask questions in a multicast session did not understand the privacy implications of that interaction. Finally, conference attendees who did not participate in the session perceived their system interaction as non-existent and thus when they realised that their images have been transmitted felt their privacy had seriously been invaded.

EXAMPLE: NON-PARTICIPANTS

“Apparently one time someone was tuning in and they saw one of my colleagues, one of my co-workers, falling asleep in one of the sessions - I fall asleep in lots of the sessions - but they [his bosses] took him to task for it, you know ‘We saw you falling asleep, we didn’t send you there to fall asleep!’ you know.”

This example also highlights issues about the relationship of the receiver to the user which then increases the sensitivity of the information. The person falling asleep *may* not have minded a stranger viewing him remotely but his boss can make valued judgements about him and his personality that can have serious repercussions on his working relationships.

Ultimately this study identified that, with regard to users’ perceptions of privacy, there should be a re-definition of the user. To assess privacy adequately, from the users’ perspective, it must be understood that it is only as an *information broadcaster* that the users’ *risk* their privacy being invaded. As an *Information Receiver* the user encounters *benefits* that can be traded off against potential *risks*. Systems distorting the balance between these two roles (making a user more of a broadcaster or receiver) can affect potential *privacy risks* and feedback required by the user to trade-off against

privacy risks. Within this study the user is primarily a broadcaster with no immediate but with potential long-sighted *benefits*. Consequently this scenario relies heavily on the users' *trust* and potential breaches to this *trust* could have serious repercussions.

Grounded Theory model building

This section partially supports the model factor:

User factor: user distinction (Sub-section 8.3.1.2)

User factor: system interaction (Sub-section 8.3.1.3)

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

Information Receiver: Trust (Sub-section 8.3.3.1)

Information Receiver: Relationships (Sub-section 8.3.3.2)

Information Receiver: Trade-off's group membership (Sub-section 8.3.3.5)

Information Usage (IU): Current IU – task (Sub-section 8.3.4.1)

Information Usage (IU): Later IU – recording awareness (Sub-section 8.3.4.2)

Information Usage (IU): Trade-off – risk / benefit (Sub-section 8.3.4.6)

Context: Technology – presence (Sub-section 8.3.5.3)

Privacy invasion cycle (Section 8.1): the importance of users initial *trust* levels is identified. These participants had an initially high trust level – if asked at the beginning of the study if there were any potential privacy problems with the technology they answered 'no'.

However, potential invasions were identified which perturbed users.

6.1.3.2 Information receiver

Many interviewees initially noted (descriptive statistics) that the *Information Receiver* (IR) was not an important issue for them: "...because the people that really matter are here, at the IETF."

Further detailed analysis of the results (using Grounded Theory) showed that these perceptions rely on some important implicit assumptions about the *Information Receiver*. Most of those interviewed assumed that the remote viewers were a smaller number of the same type of people that attended the IETF meeting, and mainly academics (because these have easier access to the Mbone). However, when the issue of *outsiders* (people not a part of the IETF technical community) remotely viewing the sessions was discussed a quarter of the respondents highlighted associated privacy problems. Interviewees were, to some degree, concerned with the possibility that *outsiders* receiving the transmissions might change the dynamics of IETF session in two ways:

1. "...it would inhibit some of the discussion."
2. "... it would encourage people to make statements with that broader audience in mind as opposed to just technical peers."

Respondents also noted that *remote viewers* might misunderstand some presentations. At the IETF meeting, attendees often clarify points in a discussion with the speaker or contributor after the session ends – remote attendees were noted as finding it hard to do this and thus were more open to misinterpreting the session and the presenter.

For most of those interviewed, however, the *benefits* of multicast sessions for community members who cannot attend the IETF meeting outweighed the potential *privacy risks* associated with sessions being viewed by *outsiders* and *remote viewers*. It is important to note, however, that the same trade-off did not apply to the hotel-internal transmission of IETF sessions.

EXAMPLE: OUTSIDERS

One interviewee recalled that the hotel in which a previous IETF had been held had transmitted sessions on its internal television network – this opened up the sessions to viewers who were not part of the IETF community, without speakers and contributors being aware of it.

Unlike remote viewing, the respondents perceived being able to view the conference via a hotel TV link-up as not important enough to outweigh the *privacy risks* of broadcasting (see example above). The study results have shown that it is vital to assess users' assumptions about the *Information Receiver* prior to distribution decisions being made. It is also important to understand privacy trade-offs so that the effects of changing circumstances can be assessed prior to users losing their trust in the organisation.

Grounded Theory model building

This section partially supports the model factor:

Information Receiver: Trust (Sub-section 8.3.3.1)

Information Receiver: Trade-off's – trust (Sub-section 8.3.3.3)

Information Receiver: Trade-off's group membership (Sub-section 8.3.3.5)

Information Usage (IU): Trade-off – risk / benefit (Sub-section 8.3.4.6)

Context: Technology – environments (Sub-section 8.3.5.1)

Context: Social groupings – social group outsiders (Sub-section 8.3.5.5)

Context: Organisational culture – trust (Sub-section 8.3.5.7)

Privacy invasion cycle (Section 8.1): the importance of users initial *trust* levels is identified.

6.1.3.3 Information Usage: recording

The recording of sessions was not initially noted (descriptive statistics) as a major issue although a quarter of participants stated that a lack of recording context (time and place) increased the chances of misinterpreting the session information. The mere recording of data was suggested as increasing the likelihood of re-using the information (in its entirety) within a different context and thus potentially its sensitivity. A session viewed 10 years later, without any temporal context cues, could produce a viewer's perception that the presenter is outdated and as such their views not worth any regard. This highlights an important interaction between the *informations' usage* and its *sensitivity*.

A key issue noted by the respondents was the recording of sessions that became *emotive* (See Sub-section 6.1.3.1). Using recorded multimedia data with *secondary level information* (such as an emotive session) increases its sensitivity, as the potential to view the data repeatedly increases. An embarrassing instance (emotional response in a debate, an indelicate physical action) within an interaction could be 'written off' as one of those humiliating moments best forgotten. However, a recording of that event can be watched an infinite number of times by numerous people.

EXAMPLE: EMOTIVE SESSION RECORDING

“Only once when I slightly lost my temper and felt more like, you know, some people, they save it and watch it later on. It's the sort of thing that you wouldn't want to be captured for ever.”

The increase in media and thus *secondary information* was identified as directly related to an increase in the information's potential invasiveness when re-used in a different context. With the recording of this multicast data, the associated *privacy risks* are higher than with, as one respondent pointed out, documented records of events:

“Although that kind of thing might not get reflected in the minutes as much - the level of emotion. I mean the argument might get reflected but the emotion won't be. How long did I yell - you know.”

Multicast and recorded conference sessions were acceptable to the majority of speakers if they were viewed within a similar context. However, when participants were questioned about *secondary level information* being assessed within a different context this was found to be unacceptable and potentially invasive e.g.

- i) Sessions used to illustrate mistakes commonly made in presentations.
- ii) Session evaluated to study the behaviour of *techies*.
- iii) Sessions reviewed to identify how people from different ethnic backgrounds act and react in an argument.

At this secondary level, the data of technical debates suddenly seemed very personal, and its *usage* perceived as highly intrusive. The key factor here is the realisation that a misjudgement has been made. The users' (*Information Broadcasters*) assessment of the *risk* involved in the situation is inaccurate, and their control of the potentially invasive material is lost (Bellotti, 1997). Although misjudgements about the potential invasiveness of information can be made in normal situations, complex problems arise when technology inadvertently supports these misinterpretations. This emphasises the importance of keeping data in its context (Dix, 1990).

Grounded Theory model building

This section partially supports the model factor:

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

Information Sensitivity: Trade-off's (Sub-section 8.3.2.4)

Information Usage (IU): Later IU – repeated viewing (Sub-section 8.3.4.3)

Information Usage (IU): Later IU – context (Sub-section 8.3.4.4)

Privacy invasion cycle (Section 8.1) the importance of users initial trust levels is noted.

6.1.3.4 Information Usage: editing

The most important *Information Usage* issue (both in terms of percentage of responses – descriptive statistics - and strength of feelings) was related to the *editing* of recorded sessions. As one respondent noted:

“It turns something into a pretty subjective interpretation of it.”

Editing of data is often a source of users' privacy fears as it is possible to maliciously misrepresent information. Privacy invasions, however, can still occur without malicious intent, when large sections of low sensitivity multimedia data are used out of context (see below).

EXAMPLE: EDITING OUT OF CONTEXT

“Somebody told me: ‘Hey, I saw you the other day. I went to this workshop on multicast technology and you were talking,’ and I said: ‘I wasn’t talking there.’ They had shown like a demo of what a typical multicast session looked like, and it happened to be my presentation, and of course I hope they didn’t show something like when I got a lot of questions or if there’d been a very heated discussion and I hadn’t been doing very well at that discussion. I’d have found it a little bit embarrassing. They would show it to this group of people who have no idea what I’m talking about, what the subject is... In fact they probably wouldn’t have listened to my whole presentation, they probably showed the last 5 minutes - a snippet - and they would have taken it completely out of context and of course that’s not good.”

The respondent (although an advocate of session recording) was concerned because a section of the data may not portray his argument accurately (when interpreted as information) for a non-technical audience thus potentially making him look ridiculous. The *Information Receiver* (who had edited this session) were probably not worried about the privacy implications of re-using this data because:

- i) The sessions were broadcast and understood to be an open forum.
- ii) They were not presenting the session snippet for its primary or secondary source information but to view the medium itself (quality, reliability etc.).

However, as the recording contains primary and secondary information they could not guarantee that someone unacceptable to the initial *Information Broadcaster* (system user) would be able to view this data and misinterpret its content.

Ultimately the majority of interviewees saw the editing of data out of context as a major privacy problem which can be highlighted by one respondent’s comments: -

“I don’t mind editing in principle – it’s just the way it seems to happen in practice that I seem to mind.”

When *low sensitivity* data is taken out of context, it can sometimes become highly sensitive, personal representational information (at the secondary level) showing the user in a bad light. This issue of

editing recorded sessions out of context increased in importance with the editing of multimedia data from emotive sessions:

“I think that could be a problem if you’re snarling at somebody and you miss all the reasons why you’re snarling at them - so making you look unreasonable.”

Grounded Theory model building

This section partially supports the model factor:

User factor: user distinction (Sub-section 8.3.1.2)

Information Sensitivity: Primary / secondary information (Sub-section 8.3.2.3)

Information Sensitivity: Trade-off’s (Sub-section 8.3.2.4)

Information Usage (IU): Later IU – editing (Sub-section 8.3.4.5)

6.2 CHAPTER SUMMARY

Due to a high level of *trust* in both the technology and organization that implemented it, these users had few initial privacy concerns. However, the interviews identified that this *trust* relies on inaccurate assumptions that could, and had already, caused their privacy to be invaded. Users who experienced an unexpected invasion of their privacy were found not only to be likely to reject the technology that afforded the invasion, but also to lose trust in the organisation that introduced it. Users’ system interaction perceptions (*information broadcaster* and receiver) also produced variations in privacy perceptions and trade-off’s. The user encountered *privacy risks* in the former role and in the latter role task interaction *benefits* that may have traded-off against those *risks*.

Various issues for all the privacy factors were verified and expanded upon. The study results corroborated previous research findings detailing the effects of primary and secondary levels on *Information Sensitivity*. Specifically emotive representations of those being transmitted increase the amount of highly sensitive secondary level information. Privacy problems were also found to occur if users believe that data is being broadcast to *Information Receivers* who are within group members when those perceived as outsiders receive the data. The data’s sensitivity greatly increased with outsiders viewing it and potentially misinterpreting it. Finally with regard to *Information Usage* simply recording data can increase its’ *Information Sensitivity* levels, especially if it is emotive data or the data has been taken out of context. Editing the data is a major source of users’ privacy fears. However, this study revealed that this may not occur maliciously but unintentionally when segments are taken out of context. Changes in the technology of transmission can have serious repercussions on perceived *Information Sensitivity* levels, especially when remote viewers are allowed to interpret the information out of important context elements.

A Grounded Theory summary of research from this Chapter is presented in Table 6.2. This representation shows how the research presented in this Chapter expands the privacy model being developed, where the gaps are currently in the model and how the following Chapter will expand on the model.

Model Factors	Chapter 6 Privacy model contributions	Factors verified and model gaps	Chapter 7 Model development
USER FACTORS		The study verified and expanded upon the user factors identified although users' privacy mental models were not fully reviewed.	Chapter 7 will identify and expand upon previously identified privacy model factors and any trade-offs that are made with variations in perceptions of the public / private situational divide.
<i>User distinction</i>	Sub-sections 6.1.3.1, 6.1.3.4		
<i>System interaction</i>	Sub-section 6.1.3.1		
INFORMATION SENSITIVITY (IS)		The primary / secondary information factor was verified with new privacy factor trade-off's identified. The private / public divide, however, was again not established.	
<i>Primary / secondary information</i>	Sub-sections 6.1.3.1, 6.1.3.3, 6.1.3.4		
<i>Trade-off's</i>	Sub-sections 6.1.3.3, 6.1.3.4		
INFORMATION RECEIVER (IR)		Previously identified information receiver issues were expanded with regard to trust and group membership. Interactions between IR and other privacy factors require further exploration.	
<i>Trust</i>	Sub-sections 6.1.1.1, 6.1.3.1, 6.1.3.2		
<i>Trade-off's - trust</i>	Sub-section 6.1.3.2		
<i>Trade-off's - group membership</i>	Sub-sections 6.1.1.1, 6.1.3.1, 6.1.3.2		
INFORMATION USAGE (IU)		Previously identified IU issues of task, recording awareness and context were expanded upon. Repeated viewing, editing and risk/benefit trade-offs were also identified. However, interactions between these IU issues and other privacy factors require further exploration.	
<i>Current IU - task</i>	Sub-sections 6.1.3.1		
<i>Later IU - recording awareness</i>	Sub-section 6.1.3.1		
<i>Later IU - repeated viewing</i>	Sub-section 6.1.3.3		
<i>Later IU - context</i>	Sub-section 6.1.3.3		
<i>Later IU - editing</i>	Sub-sections 6.1.2, 6.1.3.4		
<i>Trade-off's - risk / benefit</i>	Sub-sections 6.1.3.1, 6.1.3.2		
CONTEXT		This study expanded the model with the verification of the contextual issue of organisational trust. However, cultural and social groupings require further exploration.	
<i>Technology - environments</i>	Sub-section 6.1.3.2		
<i>Technology - presence</i>	Sub-section 6.1.3.1		
<i>Social groupings - outsiders</i>	Sub-sections 6.1.2, 6.1.3.2		
<i>Organisational culture - norms</i>	Sub-section 6.1.3		
<i>Organisational culture - trust</i>	Sub-sections 6.1.3, 6.1.3.2		
PRIVACY INVASION CYCLE	Sub-sections 6.1.3.1, 6.1.3.2, 6.1.3.3	Cycle trust factors identified	

Table 6.2: Study 4 Grounded Theory research summary, privacy model contributions and gaps

Chapter 7: Privacy invasion study

Ubiquitous multimedia applications often obscure potential privacy implications from users. Technology implementers are often dissuaded from increasing users' awareness for fear it may open a *can of worms* causing users to reject the technology. Providing adequate protection for people's privacy is also complicated in ubiquitous multimedia environments as they involve many individuals, domains and cultures. The previous study reviewed *privacy threats* in a system with participants noting occurrences where the system was starting to invade their privacy (semi-invasive). The importance of users' *trust* in the technology and organization of implementation was specifically highlighted. To fully complete the development and verification of the *privacy model* a study was required to review users' who perceived their privacy had been totally invaded. This author considered, though, that this would be either unethical¹⁹ or impractical²⁰ to complete. However, an opportunistic scenario occurred which enabled a study to be completed that could verify and expand upon the *privacy model* and factors already identified (see Study 1,2,3 and 4: Chapters 5 & 6). This opportunistic study details users' perceptions of privacy invasion due to the placement of a video camera in a departmental common room without awareness or agreement by most of the respondents. The reasons why user's trade-off perceived *privacy risks* against *benefits* was reviewed further. Relying merely on social controls for safeguarding privacy is dangerous if assumptions based on social cues are distorted by the technology itself. This study enabled a review of firstly the social norms that guide interactions and secondly how ubiquitous multimedia environments distort these norms and relevant privacy factors.

7.1 PRIVACY INVASION STUDY (study 5): INVASIVE

A small camera was initially placed in the departmental common room by a small group of departmental members (not by the thesis author) without official authorization or notification to the majority of departmental members. A notice was placed on the common room door about the presence and purpose of the camera. However, most members of the department did not read this notice as the door was always open and the notice obscured. The camera's existence was initially announced in a casual message to a small email list of multicast tool developers. A week later, a casual email message about the availability of images from the common room was sent to a larger multimedia research list, and finally to the departmental mailing list. The people who placed the camera gave three reasons for doing so:

1. "*We can see from our desks what's going on in the common room and decide whether to go there.*"
2. "*To stop people taking coffee from other people's pigeonholes*" (followed by a ";-)" smile).
3. "*This helps us gain experience with telepresence.*"

¹⁹ To devise an experiment whereby users privacy was invaded.

An email debate ensued in which several people stated they were unhappy about the camera in the common room. It was then suggested that the camera would be more beneficial in the photocopier room to check the accessibility of the copier. After one day of emotive email debate, the camera was moved to the photocopier room. There was a prominent notice on the photocopier room door and an announcement on the multimedia research list. The email debate continued, and further objections were raised, until the camera was finally removed altogether after a few days.

7.1.1 Method

The small unobtrusive camera initially captured a limited view of the common room, including the entrance, pigeonholes (where mail is placed) and some of the seating area (see Diagram 7.1). A later placement of the camera, behind the copier, in the photocopy room transmitted a close-up view (at hip level) of people using the photocopier.

The camera transmitted low-bandwidth (10-24kbs) video only to the permanent multicast session “Places all over the World”. The session did not have restricted accessibility and thus could be viewed by anyone connected to the Mbone anywhere in the world.

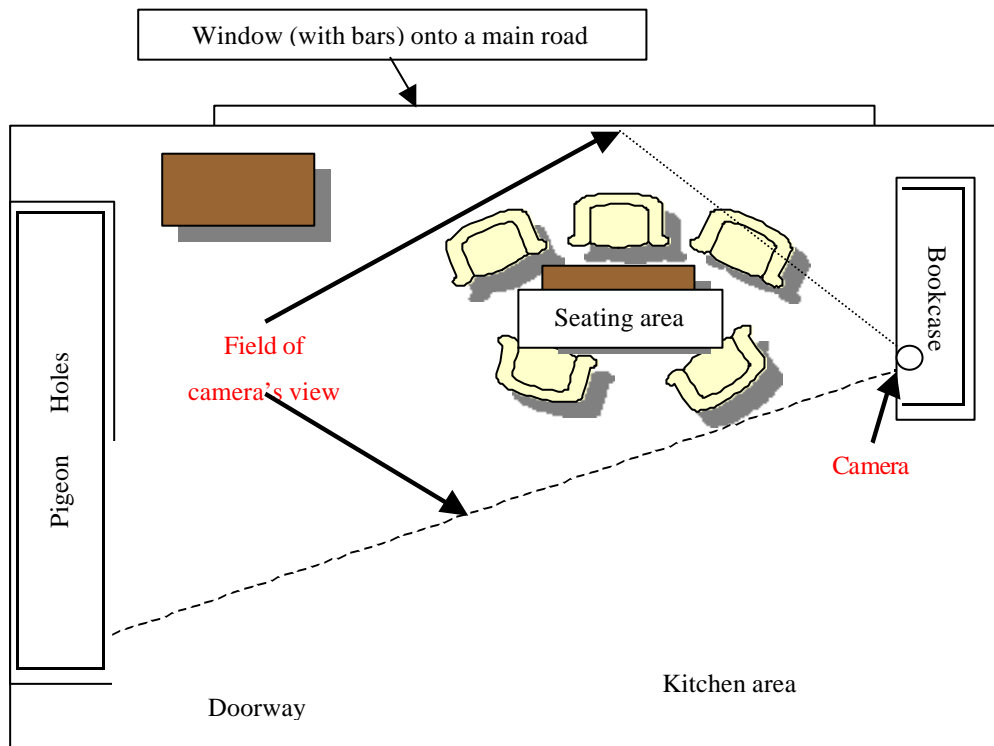


Diagram 7.1: Plan of the CS common room as viewed by the camera

²⁰ Searching the world for cases of privacy invasion that could immediately be investigated in-depth.

7.1.1.1 Participants

Participants in this study were members of the department who completed a questionnaire or took part in the email debate. Although many members of the computer science department have extensive knowledge of, and experience with, computers, they ranged from experts to novices with regard to multimedia communications. As the questionnaire data did not identify demographic details²¹, for privacy protection purposes, it is not possible to break down specifically the relation of the sample to the departmental population. From the email debate data, however, it is possible to infer that approximately a third of the respondents were multimedia communication experts. It was also possible to identify that it was these participants who initially placed the camera in the common room.

7.1.1.2 Study procedure

The camera placement in the common room and the ensuing email debate both preceded the instigation of this study. A 2-page anonymous paper questionnaire (see Appendix 2), containing both closed and open-ended questions²², was distributed to all departmental members via their pigeonholes. The questionnaire asked how comfortable users were about:

- (a) audio and video transmission;
- (b) the situation (common vs. photocopier room);
- (c) different levels of transmission (department vs. university vs. world);
- (d) the re-use of the data within a different context.

Members of the department who participated in the email debate were contacted and asked if they had any objections to their comments being used within this study. They were assured that the responses would be anonymous and the data treated in confidence. As there were no objections to the study proceeding the ensuing email debate (qualitative data), and 47 anonymous questionnaire responses (qualitative and quantitative data), were analysed in depth using Grounded Theory analysis.

7.1.2 Results: high level analysis

With the 47 questionnaire responses an initial quantitative analysis was undertaken. Pearson's correlation coefficient was used to identify any significant privacy related factors (see Appendix 1). There were three significant findings identified from the initial analysis. The majority of respondents agreed on two points (see Table 7.1):

1. They were significantly less comfortable with *audio* rather than *video* data being transmitted - both generally and in the specific situation of the common room (column findings 1 & 2).
2. They were significantly less comfortable with the *re-use* of (recorded) video data as opposed to continuous transmission within the specific situation of the common room (column finding 3).

²¹ This data could have been perceived as potentially able to track respondents (e.g. multimedia expertise, sex)

	Variables	No of respondents	Mean	Sig
1	General Visual & Audio	47	3.10 4.619	P < 0.005
2	Specific* Visual & Audio	47	3.17 4.643	P < 0.005
3	Specific* Visual & Reuse	47	3.17 4.24	P < 0.005

Table 7.1: Significant findings for all respondents (*specific situation of the common room)

Further analysis identified that clusters of respondents were counteracting strong perceptions. This meant that a group that felt their privacy was not being invaded was counterbalancing a group that felt their privacy was being invaded. A cluster analysis identified 3 groups with significantly different *perception profiles* identified by further t' tests (see Table 7.2 and Diagram 7.2)

	Grp 1	Grp 2	Grp 3
Group size	15	14	13
Significance levels (P values)			
Visual transmission General and Specific (situation)	.029*	.655	.053
General Visual and Audio	.005*	.000*	.000*
Specific Visual and Audio	.055	.000*	.000*
CS and UCL (distribution)	.189	.047*	1.000
CS and World (distribution)	.096	.028*	.721

Table 7.2: Clustered groups comfort levels (*P<0.05)

7.1.3 Results: detailed analysis

Using Grounded Theory, the quantitative analysis and further qualitative analysis melded together to provide distinct profiles for each group (see Table 7.3, 7.4 and Appendix 1). The qualitative issues were categorized according to the 3 privacy factors highlighted within the previous studies (see Chapters 5 and 6: *Information Sensitivity, receiver and usage*).

²² These sections allowed respondents to let off steam – several pages were sometimes added to the questionnaire – and provided a rich form of qualitative data.

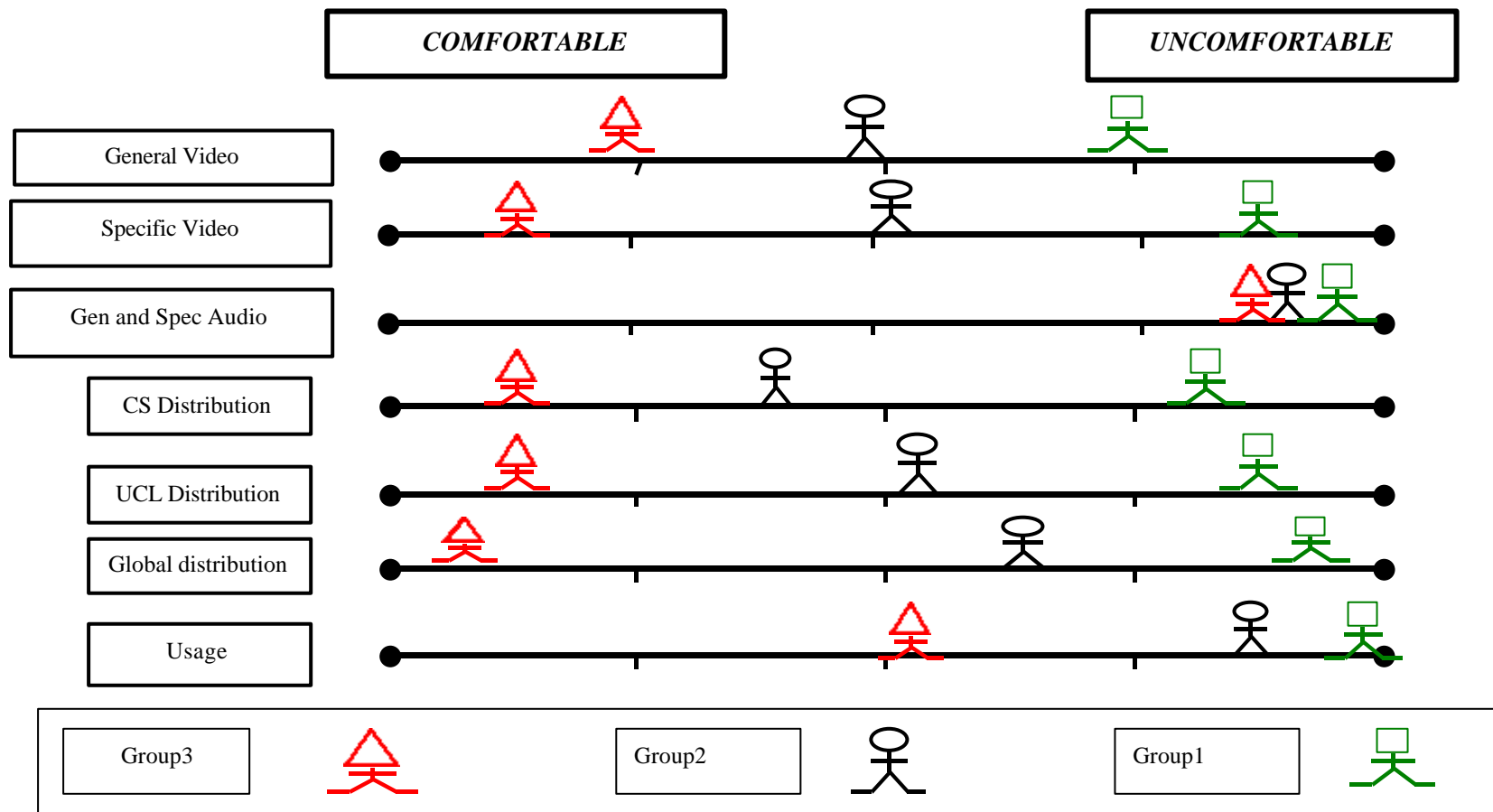


Diagram 7.2: Group profile for relevant privacy issues

Grounded Theory enabled properties and dimensions of the privacy factors to be identified (e.g. *Information Sensitivity* / property: common room situation / dimension: private – public). The frequency that these properties at the dimensional level occurred was recorded and compared for each of the groups (see Table 7.3). A clear difference was identified between group 3’s perspective of the situation as public, having observer control and benefits from the technology compared to the other two groups. From Table 7.2 and Diagram 7.2 we can also see that group 3 members were most comfortable with the current camera placement scenario (see Appendix 1).

	Grp 1	Grp 2	Grp 3
Information Receiver (broadcaster)			
Perceived Observed lack of Control	9	5	0
Perceived Observer Control	0	0	7
Information Sensitivity			
Common Room Private Situation	3	4	1
Common Room Public Situation	0	0	4
Information Usage			
Benefits	0	6	7
Risks	14	8	0

Table 7.3: Sample of qualitative analysis by groups (frequency data)

Since questionnaire responses were anonymous²³ no further quantitative analysis of group 3 members was possible. However, analysis of the email debate identified that some of the email respondents (multicast tool developers - who had placed the camera in the common room) exhibited group 3 profiles.

	Groups 1 & 2	Group 3
Perceived Observed lack of Control	<i>“... how to become one of the peeping toms”</i>	No comments
Observer Control	No comments	<i>“Could also be used as a soap substitute”</i>
Emotive response	<i>“Only for nosy computer scientists wishing to assess the usefulness of their technology.”</i>	No comments

Table 7.4: Sample of coded comments

²³ due to the opportunistic nature of the study and to protect respondents privacy

Grounded Theory model building

This section partially supports the model factor:

Information Usage (IU): Trade-off – risk / benefit (Sub-section 8.3.4.6)

Context: Social groupings – social groups (Sub-section 8.3.5.2)

7.1.3.1 User factor

In study 4 (see Chapter 6) an important privacy distinction²⁴ was identified between the *information broadcaster* and *receiver*. It is as an *information broadcaster* that users' experience *privacy risks* with data transmission but as *receivers* these can sometimes be traded-off against potential *benefits*. Potential problems with privacy invasion are increased if an environment ascribes the user to only an *information-broadcaster* only role (see Sub-section 8.3.1.2).

It is interesting to note that the camera deployers stated that one of the purposes for the technology was to increase the department's telepresence and allow observers to judge the accessibility of the common room. However, as the web-site location was not initially advertised to the whole department, this assigned many of the common room users to only the role of *information broadcasters*.

The third purpose behind the camera placement, detailed by the deployers in an email, was primarily for those of the *Information Receiver* and not those who were only *Information Broadcasters*. With a security motivation (catch those who take other people's coffee) behind the camera placement the camera deployers dangerously crossed the line between multi-media environments and CCTV. Crossing this line breaks many implicit assumptions that underlie respondents' multimedia environment perceptions as a tool for increased co-operation, communication and thus *freedom of information*.

The Grounded Theory analysis (see Appendix 1) revealed that all of these factors decreased the information broadcasters' sense of control over the technology and produced an emotive rejection of it beyond the confines of the present situation.

Grounded Theory model building

This section partially supports the model factor:

User factor: user distinction (Sub-section 8.3.1.2)

Information Usage (IU): Later IU – recording awareness (Sub-section 8.3.4.2)

Information Usage (IU): Trade-off – risk / benefit (Sub-section 8.3.4.6)

Context: Technology – environments (Sub-section 8.3.5.1)

Context: Technology – presence (Sub-section 8.3.5.3)

²⁴ A similar principle was established by Grudin (1988) in "why CSCW applications fail: problems in the design and evaluation of organizational interfaces"

7.1.3.2 Information Sensitivity

One pivotal finding of this study is the impact that users' perception of *Information Sensitivity* has on their assessment of privacy invasions. All users were significantly less comfortable with audio rather than video data being transmitted – what they say is potentially more sensitive than what they do, in general and in the context of the common room.

A further *Information Sensitivity* problem was identified as due to users' and technology deployers' different perceptions of the common room's *Information Sensitivity*. Groups 1 and 2 perceived that they were being observed in a *private* situation (the common room) – a violation of a social (cultural) norm. Group 3 (later identified as mainly the technology deployers) in contrast perceived the common room to be a *public* situation with reduced social norms on observing people. This finding emphasises the importance of the perceived distinction between private and public, and the expected social norms in each situation, when defining *Information Sensitivity* (Schoeman, 1992). This discrepancy in situation perceptions resulted in Group 3's high degree of *trust* (high usage *benefits* and no *risks*) in the system, whilst the rest, Groups 1 and 2 (68% of the respondents), expressed a lack of *trust* in the system (high usage costs).

Finally the individual's need to control how others view them cannot be ignored. The degree of invasiveness of the video data was identified as related to the quality and focus of the picture being transmitted. Several respondents objected to the second situation (in the photocopy room) because the camera showed the hip part of a person only - producing a potentially comical or embarrassing image. All of these results suggest that how we are viewed depends on the situation in which we are observed. *Information Sensitivity* is therefore closely related to the situation from which data is transmitted.

Grounded Theory model building

This section partially supports the model factor:

Information Sensitivity: Judgement (Sub-section 8.3.2.1)

Information Sensitivity: Public / private situation (Sub-section 8.3.2.2)

Information Receiver: Trust (Sub-section 8.3.3.1)

Information Receiver: Trade-off's group membership (Sub-section 8.3.3.5)

Information Usage (IU): Trade-off – risk / benefit (Sub-section 8.3.4.6)

Context: Social groupings – social groups (Sub-section 8.3.5.2)

Context: Social groupings – social group outsiders (Sub-section 8.3.5.5)

Context: National and international – cultural norms (Sub-section 8.3.5.8)

7.1.3.3 Information receiver

Contrary to our expectations, the majority of respondents did not perceive variations in the *Information Receiver* as an important factor effecting *Information Sensitivity*. However, group 2 did find the distribution of the visual data beyond the department to be significantly more uncomfortable than within the department. Ultimately, the two groups that did not perceive the *Information Receiver* as a factor, either perceived the data as highly sensitive and thus invasive

regardless of who viewed it (group 1) or very low in sensitivity and non-invasive whoever saw it (group 3). This clearly highlights how *Information Sensitivity* judgements can affect the importance of who sees the data.

Grounded Theory model building

This section partially supports the model factor:

Information Receiver: Relationships (Sub-section 8.3.3.2)

7.1.3.4 Information Usage

All of the respondent's expressed strong discomfort if the video data transmitted in this study was to be recorded and re-used (*Information Usage*) out of context (Dix, 1990). This highlights the flexible nature of *Information Sensitivity* - data initially considered to be non-invasive may be perceived as invasive when used out of context. However, it must be noted that within this study it is the transmission of debatably sensitive data that has invaded privacy. The recording or re-usage of this data aggravated already sensitised perceptions of it.

Grounded Theory model building

This section partially supports the model factor:

Information Usage (IU): Later IU – repeated viewing (Sub-section 8.3.4.3)

7.1.3.5 Context

This study revealed that users' assessment of a situation depends on the degree of *control* they retain over how they are viewed and by whom. The results identified that the observer's *control* of the technology distorted their perception of the *place* as through the eyes of an observer rather than as one being observed. To explain this complex phenomenon, consider the analogy of sitting in a café (semi-private) watching people in the street (public) - which is socially acceptable in most cultures. However, someone in the street (public) pulling up a chair and staring in at the diners of the café (semi-private) would be perceived as unacceptable. Relating this analogy to this study we can understand that the common room users' perceived the situation as their café (semi-private) looking out on the street and corridor (public), able to see who can see them. The common room observers, however, are sitting at their desk – equivalent to their café - (private) looking out on the common room (what they considered as public), seeing people who cannot see them. The issue highlighted by this example is the perceived ownership and control of the *window*. We know and accept the *risk* of being watched and scrutinized as we walk in the streets (public). However, in more private situations (e.g. a café or changing room) our acceptance of being watched is reduced. It could therefore be argued that Group 3's perception of the common room as public is connected to their perspective of *observing*²⁵ rather than *being observed* in this situation (Group 1 & 2's assessment).

²⁵ These respondents, also frequently used the common room and commented on this factor.

It is interesting that those who originally placed the camera (technical experts in network multimedia) showed Group 3 profiles in the email discussion. A sense of being in *control* of the technology could therefore be linked to a distorted perception (from the majority) of the situation. The key to their distorted assumptions of the situation, as being public, was their familiarity with the multimedia tools and thus their sense of control over the technology. This is probably why, even though Group 3 people also used the common room, their over-riding perception of the situation was that of an observer i.e. even when present in the common room they are looking ‘through the camera’s eyes’.

Grounded Theory model building

This section partially supports the model factor:

User factor: system interaction (Sub-section 8.3.1.3)

Information Sensitivity: Public / private situation (Sub-section 8.3.2.2)

Information Usage (IU): Later IU – context (Sub-section 8.3.4.4)

7.1.3.6 Emotive backlash

Ultimately, our behaviour is guided by the situation. If we misjudge the situation then we are at more of a *risk* of socially embarrassing ourselves. Assessing that situation is, therefore, of immense importance in our social interactions. This may help us to explain the emotive response that ensued from the camera installation: a perceived privacy invasion. The emotive response could be argued to be caused by group 1 & 2’s perceived *lack of control* over the situation, whereas group 3 could not understand what all the fuss was about. The camera deployers’ (group 3’s) surprise at the emotive response to the perceived privacy invasion showed how they had made inaccurate assumptions and thus misinterpreted the situation. Emotive privacy responses are a defence mechanism to a perceived threat, resulting from a lack of control over - potentially detrimental – representations of the self (Goffman, 1969; Schoeman, 1992). Once users’ experience a lack of *control* and respond emotively, a total rejection of the application and all similar technology is the likely consequence. In this study, those who felt the most discomfort subsequently rejected transmission of any audio and video data under any circumstances.

The different perceptions identified within this study may have already existed within the department. However, introduction of this technology brought these differences to the fore, resulting in tension and an emotive debate which ended with a formal departmental decision to remove it. This is a lesson for other organisations: to assess how the relationships between organisational control and trust will affect users’ privacy. Trust can be undermined if users are not allowed to judge trade-offs for themselves or feel part of the proposed solution (Goffman, 1969; Schoeman, 1992). Guidelines and boundaries (rather than restrictive controls) for the technology are required to encourage and nurture trust.

Grounded Theory model building

This section partially supports the model factor:

Information Receiver: Trust (Sub-section 8.3.3.1)

Information Receiver: Trade-off's group membership (Sub-section 8.3.3.5)

Context: Organisational culture – trust (Sub-section 8.3.5.7)

Context: Organisational culture – organisational norms (Sub-section 8.3.5.6)

Privacy invasion cycle (Section 8.1): The importance of users *emotive* response to privacy invasion is identified – this provides the motivation behind the cyclic nature of the cycle (e.g. ever decreasing trust).

7.2 CHAPTER SUMMARY

Various issues for all the privacy factors were verified and expanded upon with the findings from this study. With regard to *Information Sensitivity* the findings highlighted the importance of what media type of data is transmitted (audio or video), what images are transmitted (camera at hip-height in the common room) and from what situation (public or private) it is transmitted. The majority considered it a private situation whilst a small group (identified later as primarily the technology deployers) perceived the situation as public. The groups differed in the perceived *control* exerted by observers and those observed. It is argued that initially different perceptions in technology control produced different perceptions of the situation as public or private. Those that felt observed in this situation and without control of the technology became emotive about the camera placement and what subsequent action should occur.

The privacy factor *Information Receiver* and *Information Usage* were noted but not in as much detail as in previous research. It could be argued that this is because the majority of respondents felt the information sensitive and invasive regardless who saw it and what was done with it.

This study identified a privacy critical boundary beyond which users emotively reject the technology. Results from this Study have serious implications on how technology should be introduced within an organization. It is vital that the situation and implicit assumptions are judged accurately *prior* to installation of ubiquitous multimedia technology and before users lose trust and become emotive. Ultimately the results from this Study and Study 2 and 4 (Chapters 5 and 6) show that previous definitions of privacy have overlooked time factors. Users' perceptions are influenced by a number of interacting factors, which are further complicated by those factors being continually reviewed, appraised and re-evaluated with reference to each other.

A Grounded Theory summary of research from this Chapter is presented in Table 7.5. This representation shows how the research presented in this Chapter expands the privacy model being developed and how the following Chapter will integrate them in the model.

Model Factors	Chapter 6 Privacy model contributions	Factors verified and model development	Chapter 8 Model
USER FACTORS		The study again verified and expanded upon the user factors identified although users' privacy mental models were not fully reviewed.	Chapter 8 will integrate the previous literature with findings from chapters 5, 6 and 7 into a model of users' perceptions of privacy in multimedia communications. The high-level storyline of this model will be presented as the 'privacy invasion cycle'.
<i>User distinction</i>	Sub-section 7.1.3.1		
<i>System interaction</i>	Sub-sections 7.1.3.1, 7.1.3.5		
INFORMATION SENSITIVITY (IS)		IS judgement factors were verified along with the private / public divide for a privacy invasion scenario.	
<i>IS Judgements</i>	Sub-section 7.1.3.2		
<i>Public / private situation</i>	Sub-sections 7.1.3.2, 7.1.3.5		
INFORMATION RECEIVER (IR)		Previously identified information receiver issues were expanded with regard to a privacy invasion scenario. Interactions between IR and other privacy factors were also reviewed.	
<i>Trust</i>	Sub-sections 7.1.3.2, 7.1.3.6		
<i>Trade-off's - group membership</i>	Sub-sections 7.1.3.2, 7.1.3.6		
INFORMATION USAGE (IU)		Previously identified IU issues of recording awareness, repeated viewing and context were expanded upon for a privacy invasion scenario. Risk/benefit trade-offs were also identified between these IU issues and other privacy factors.	
<i>Later IU - recording awareness</i>	Sub-section 7.1.3.1		
<i>Later IU - repeated viewing</i>	Sub-section 7.1.3.4		
<i>Later IU - context</i>	Sub-section 7.1.3.5		
<i>Trade-off's - risk / benefit</i>	Sub-sections 7.1.3, 7.1.3.1, 7.1.3.2		
CONTEXT		This study verified and expanded upon all the contextual issues (except interface issues) for a privacy invasion scenario.	
<i>Technology - environments</i>	Sub-section 7.1.3.1		
<i>Technology - presence</i>	Sub-section 7.1.3.1		
<i>Social groupings - social groups</i>	Sub-sections 7.1.3, 7.1.3.2		
<i>Social groupings - outsiders</i>	Sub-section 7.1.3.2		
<i>Organisational culture - organisational norms</i>	Sub-section 7.1.3.6		
<i>Organisational culture - trust</i>	Sub-section 7.1.3.6		
<i>National and international cultural norms</i>	Sub-section 7.1.3.2		
PRIVACY INVASION CYCLE	Sub-section 7.1.3.5	Cycles' emotive rejection factors identified	

Table 7.5: Study 5 Grounded Theory research summary and model contributions

Chapter 8: Privacy model

Privacy, as with trust, relies on how we perceive it and so to develop appropriate privacy mechanisms and policies we need to identify how users perceive privacy. This thesis has, therefore, sought empirically to detail a model of users' perceptions of privacy within multimedia communications. This Grounded Theory model was developed inductively from an integrated analysis of previous privacy literature and further studies of the phenomenon within multimedia communications. The model was identified, developed and conditionally verified via systematic data collection and analysis. A theory was not fabricated and then proved but instead allowed to emerge from what is relevant within the area of study. The development of the model is charted throughout the thesis by the means of:

- i) Section summary boxes stating aspects of the model that are substantiated by that section.
- ii) Chapter summaries identifying model contributions, gaps and further developments required.

Below in Table 8.1 is an outline of the chapter summaries detailing the models development:

Chapter	Extending the model	Gaps in the model
2	Aspects of all the privacy model factors are identified	There is little research on factor interaction for multimedia environments and thus context specific trade-offs that users may make.
3	Aspects of all the privacy model factors are identified for multimedia communication environments	Some previous research is not evaluated within a multimedia environment. An appropriate research method to develop a privacy model is also required.
4	Grounded Theory is the appropriate methodology to build a model for a complex phenomenon using a mixture of data and producing suitable design recommendations.	There is little previous Grounded Theory research within the domain of HCI, and none with multimedia communications, upon which to base this research.
5	Most model factors are identified and verified for multimedia communication environments. The awareness element in the privacy invasion cycle is identified.	The privacy model factors and potential trade-offs require further investigation for variations in users' <i>system interaction</i> (i.e. direct or indirect system interaction) and <i>organisational trust</i>
6	Most model factor variations are noted for different <i>system interaction levels</i> and <i>organisational trust</i> . The trust element in the privacy invasion cycle is identified.	The privacy model factors and potential trade-offs require further investigation for variations in perceptions of the <i>public / private situational divide</i> .
7	Most model factor variations are noted for the <i>public / private situational divide</i> . The emotive rejection element of the privacy invasion cycle is identified	The model requires an integration of previous literature with findings from the thesis current research. A high-level storyline of this model is also required.

Table 8.1: Development of the privacy model through the Chapters.

The Grounded Theory analysis has produced:

- 1) A *privacy model* of the factors involved in privacy invasions
- 2) A high-level story line of the model incorporating process effects (*privacy invasion cycle*) which identifies why multimedia communication systems produce privacy invasions and thus how they can be rectified.

Designers and organisations should review this *privacy model*²⁶ for specific pre-emptive solutions to reduce the likelihood of the *privacy invasion cycle* occurring.

8.1 PRIVACY INVASION CYCLE

The core category for the *privacy model* is the concept of *privacy invasion* and its story-line (the conceptualisation of a descriptive narrative for privacy invasion) is the *privacy invasion cycle*. The story-line is, itself, a process effect which means that it reports on factors that change over time. The changing process detailed in the *privacy invasion cycle* details users' strategies for managing and responding to privacy invasions (see Sub-section 4.2.1 for Grounded Theory method review).

All of the model factors and subsequent issues relate to the *privacy invasion cycle* and can produce an invasion of privacy by invoking the privacy invasion cycle.

8.1.1 Privacy invasion cycle detailed

Mackay (1995) states that professional ethics should ensure that multimedia data is used within acceptable boundaries. As multimedia communications become more complex so does the data being transmitted. It must be understood that, however, that professional's perception of transmitted data may be distorted from that of users. Consequently it is vital to identify user's perceptions and how technology, mediating interactions, distorts users' assumptions.

All the findings in this thesis (see Chapters 5, 6 & 7) have concluded that the majority of privacy invasions do not occur through malicious intent. Most invasions of privacy occur because of the *realisation* that a mismatch has occurred between their perceptions and reality. Initially users' perceptions of what data is being released mismatches with what information the *Information Receiver* (IR) is actually interpreting. However, it is the *realisation* that their original perceptions were inaccurate which produces the perceptions of privacy invasion. It is vital therefore to identify what users' perceive *Information Receivers* are receiving and interpreting as the information. The *privacy invasion cycle* (Diagram 8.1) identifies what perceptions it is important to elicit and how technology mediated interactions can contribute to privacy invasions.

²⁶ Some model aspects require further research to detail pre-emptive solutions to the *privacy invasion cycle*.

1) TRUST (see Sub-sections 6.1.3.1, 6.1.3.3): Users do not approach every situation ready to assess the *privacy risks* and *benefits* of that information exchange. The degree of *trust* felt by the user in the *Information Receiver*, technology and technology deployers determines the degree of privacy evaluation required. It is important to note that when obtaining users' privacy perceptions their responses may reflect their *trust* in the organisation rather than perceived potential *privacy risks* and responses to those *risks*. It is therefore important to obtain users' perceptions of their trust in the organisation, technology, and *Information Receivers* in order to identify how much they expect to deal with privacy protection themselves.

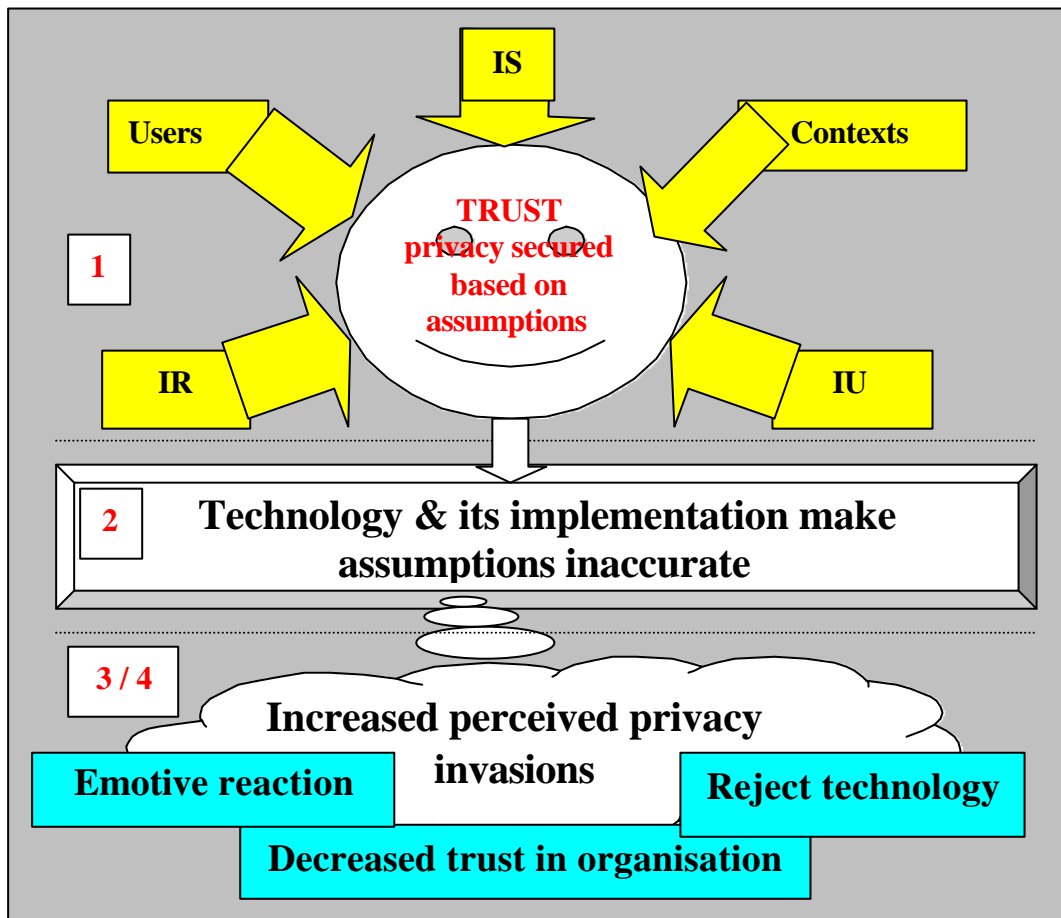


Diagram 8.1: Privacy Invasion Cycle

- 2) ASSUMPTIONS: (see Sub-sections 5.2.3.1, 5.2.3.2, 5.3.2.1, 5.3.2.4) The *trust* felt by the user in that information exchange relies, however, on many implicit assumptions surrounding that interaction.
- i) Users' previous knowledge and experiences.
 - ii) Perceived *Information Sensitivity*.
 - iii) *Information Receiver*.
 - iv) *Information Usage*.
 - v) *Context of interaction: Information, Task, Situation and Technology*.

- 3) The technology mediating the multimedia interactions, and its implementation, can make those assumptions inaccurate.
- 4) REALISATION AND RESPONSE (see Sub-section 7.1.3.6): When users realise that their assumptions are inaccurate their responses are emotive (rather than rational). They perceive an increase in privacy invasions, with a potential rejection of the technology and a decreased trust in the *Information Receiver*, the technology and the organisation implementing the technology.
- 5) DECREASING CYCLE (see Sub-section 7.1.3.6): The next time the user encounters what they perceive to be a similar scenario (i.e. similar *Information Receiver*, technology or organisation implementing the technology) their initial trust levels will be lowered, and distorted negative assumptions may prevail which if confirmed will decrease users' trust still further.

Grounded Theory thesis verification

- **Study 2:** Sub-sections 5.2.3.1, 5.2.3.2
- **Study 3:** Sub-sections 5.3.2.1, 5.3.2.4
- **Study 4:** Sub-sections 6.1.3.1, 6.1.3.3
- **Study 5:** Sub-section 7.1.3.6

Designers and organizations wishing to implement multimedia communications must identify user assumptions and match them to what is actually occurring in order to identify areas where there may be potential threats to privacy. This must occur prior to, or during, technology installation.

To counteract this *cycle* we need to:

- 1) Identify assumptions users make in multimedia communications (see users' assumptions in Tables 8.2 to 8.14).
- 2) Identify how technology or its implementation makes these assumptions inaccurate (see how technology breaches assumptions, with examples, in Tables 8.2 to 8.14).
- 3) Provide preemptive solutions to the *privacy invasion cycle* (see proposed solution in Tables 8.2 to 8.14).
 - i) Appropriate codes of practice or guidelines.
 - ii) Mechanisms for appropriate control and feedback.

The following model details potential key assumptions related to privacy perceptions that a multimedia communication system is likely to, and has, breached.

8.2 PRIVACY MODEL: A HIGH LEVEL DESCRIPTION

A model (see Diagram 8.2) of **users' perceptions** within multimedia communications has been developed based on this thesis' research (see Chapters 5, 6 and 7) and previous research (see Chapters 2 and 3) using Grounded Theory methods (see Chapter 4). It is important to note that this model is an abstract representation of important factors which will change importance with the context (e.g Context1: Information Usage > Information Sensitivity or Information Receiver, Context2: Information Receiver > Information Usage or Information Sensitivity). Similarly each *factor* can change the importance of another factor (e.g. Context3: Information Usage & thus Information Sensitivity > Information Receiver). As this thesis seeks to identify both substantive and methodological knowledge that will be both accessible and applicable for designers (see Sections 1.3 and 4.1) the models application takes a 'grounded design' (Cockton, 1999) approach (see Section 8.4)

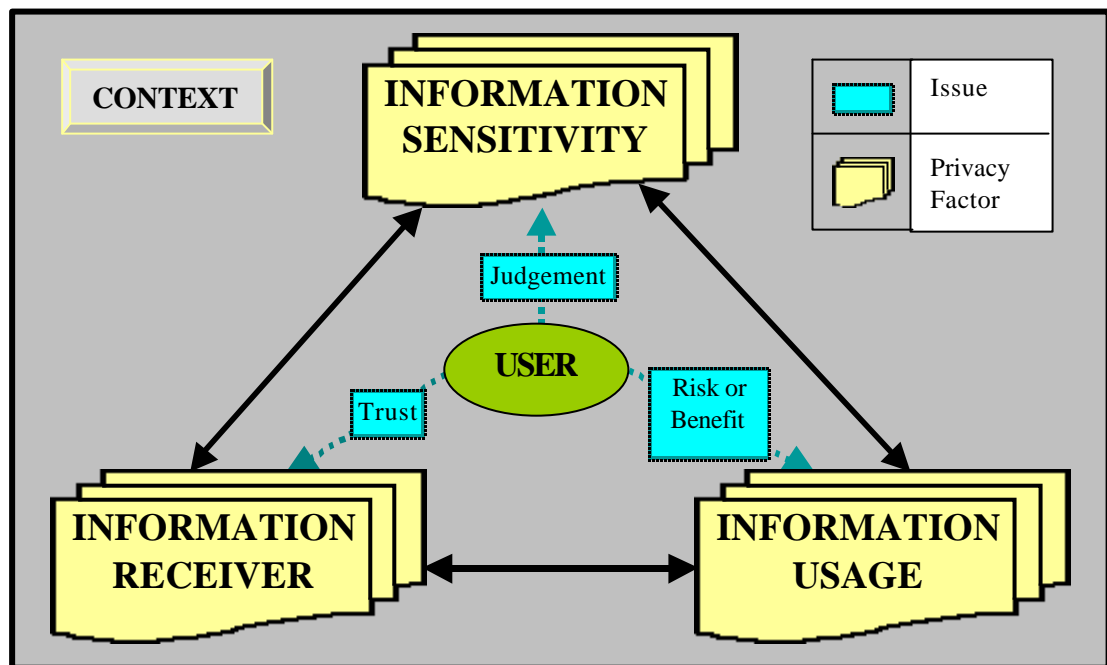


Diagram 8.2: Model summary: Users' privacy perceptions

This model presents the *User*²⁷ as the person (see *Information Broadcaster* Sub-section 8.3.1.2) who has data transmitted either directly (*primary information* - their work achievements, consumption habits, medical records etc.) or indirectly (secondary information – personality, attentiveness, intelligence) about themselves. The user may well not be actively using the system and may actually be unaware that their data (their image, voice etc.) is being transmitted (see Chapter 6 & 7). The model (Diagram 8.2) has identified 3 major privacy factors (*Information Sensitivity, Receiver & Usage*) that are key to users' perceptions of privacy. Each of the privacy factors interacts with each other to form the users' overall perception of privacy. Within different scenarios one factor will be more important than the others although all factors will effect the overall privacy perception.

²⁷ The HCI equivalent is the system end-user whereas political scientists would say the data subject.

The primary privacy factor in this model is *Information Sensitivity* (IS) and the effect that the other privacy factors have on perceived sensitivity levels. Previous data-centric approaches to privacy have concentrated on the data and not the users' perception of it. It is therefore important to understand that *Information Sensitivity*, as with privacy, relates to the users' perceptions of the data being transmitted. There are two further points to make about *Information Sensitivity*: firstly it relies on the users' judgements of the sensitivity levels of the information being broadcast and secondly that sensitivity levels are not binary (private or not private) but dimensional with degrees of sensitivity.

The *Information Receiver* (IR) is the user's perception of the person who receives and or manipulates their data. This is not necessarily the actual *Information Receiver* or manipulators. A range of issues will influence the user's assessment of the *Information Receiver*, however *trust* (often based on relationships and information roles) is an important issue in the user's *Information Receiver* perceptions.

Finally *Information Usage* (IU) relates to the user's perception of how their transmitted data is used both during the transmission and later on. The importance that the user attributes to the perceived usage is key in *privacy risk or benefit trade-offs* that are made. Like most HCI issues privacy is set within its surroundings and therefore the user's perception of the *context* within which multimedia communications occur - specifically the technology, social groupings and national or international settings - are summarised in the model. However, it must be noted that these are only a guide and relate strongly to the application of the model.

8.3 PRIVACY MODEL: A LOW LEVEL DESCRIPTION

Users' make trade-offs at the sub-factor level which affect how invasive, and thus important, the user perceives decreased privacy to be. All the *privacy model* interactions occur within a context, which must also be understood

- *USER*
 - Mental models (experience etc.)
 - Information broadcaster or receiver
 - Direct or indirect system interaction

- *Information Sensitivity*
 - Information sensitivity judgements
 - Public or private situation
 - Primary and secondary information
 - Trade-off's

- *Information Receiver*
 - Trust levels
 - Relationships
 - Trade-off's (roles, group membership)

- *Information Usage*
 - Current information usage (task)
 - Later information usage (recording, editing)
 - Trade-off's (information exchange, long term benefits)

- *Context*
 - Technology (environments, interface usability)
 - Social grouping (social norms, social groups)
 - Organisational culture (organisational norms, organisational trust)
 - National and international boundaries (cultural norms)

8.3.1 Privacy model: user

The user is a person who transmits information about themselves either directly or indirectly.

8.3.1.1 Mental models

User's personal experiences and knowledge will affect *Information Sensitivity* judgements. Mismatches between experiences and the technology can cause the *privacy invasion cycle* (Table 8.2).

<p><u>Grounded Theory thesis verification</u></p> <ul style="list-style-type: none"> • Previous literature (general & HCI): Section 2.1 Sub-sections 2.1.1, 3.2.2

PRIVACY INVASION CYCLE EXAMPLE			
Users' assumptions	Users assume that applications replicating their experiences of real-world scenarios also replicate real world privacy scenarios and protections.		
Technology breaches assumptions	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">However the technology is not only limited in what is replicated but can also provide the <i>Information Receiver</i> with more data than they would receive in the real world often without feedback to the user.</td> <td style="width: 50%;">e.g. Within VR situations people do not have proximity awareness as they would have in the real world (see Sub-section 5.3.2.4). Within many video conferencing applications the user can zoom in on images without the <i>information broadcaster</i> knowing, whereas in the real world it would be obvious if someone was staring at you - getting closer. (see Sub-section 5.2.2.3 & 7.1.3.1)</td> </tr> </table>	However the technology is not only limited in what is replicated but can also provide the <i>Information Receiver</i> with more data than they would receive in the real world often without feedback to the user.	e.g. Within VR situations people do not have proximity awareness as they would have in the real world (see Sub-section 5.3.2.4). Within many video conferencing applications the user can zoom in on images without the <i>information broadcaster</i> knowing, whereas in the real world it would be obvious if someone was staring at you - getting closer. (see Sub-section 5.2.2.3 & 7.1.3.1)
However the technology is not only limited in what is replicated but can also provide the <i>Information Receiver</i> with more data than they would receive in the real world often without feedback to the user.	e.g. Within VR situations people do not have proximity awareness as they would have in the real world (see Sub-section 5.3.2.4). Within many video conferencing applications the user can zoom in on images without the <i>information broadcaster</i> knowing, whereas in the real world it would be obvious if someone was staring at you - getting closer. (see Sub-section 5.2.2.3 & 7.1.3.1)		
SOLUTION	Identify how virtual replication of real world scenarios exceeds or limits privacy protection. Provide user with threat feedback for data potentially sensitive (see IS).		

Table 8.2: Users' experience and the *privacy invasion cycle*

8.3.1.2 User distinction

Within most multimedia interactions (with a system or another user) a user is both an *information broadcaster and receiver*²⁸ (Diagram 8.3).

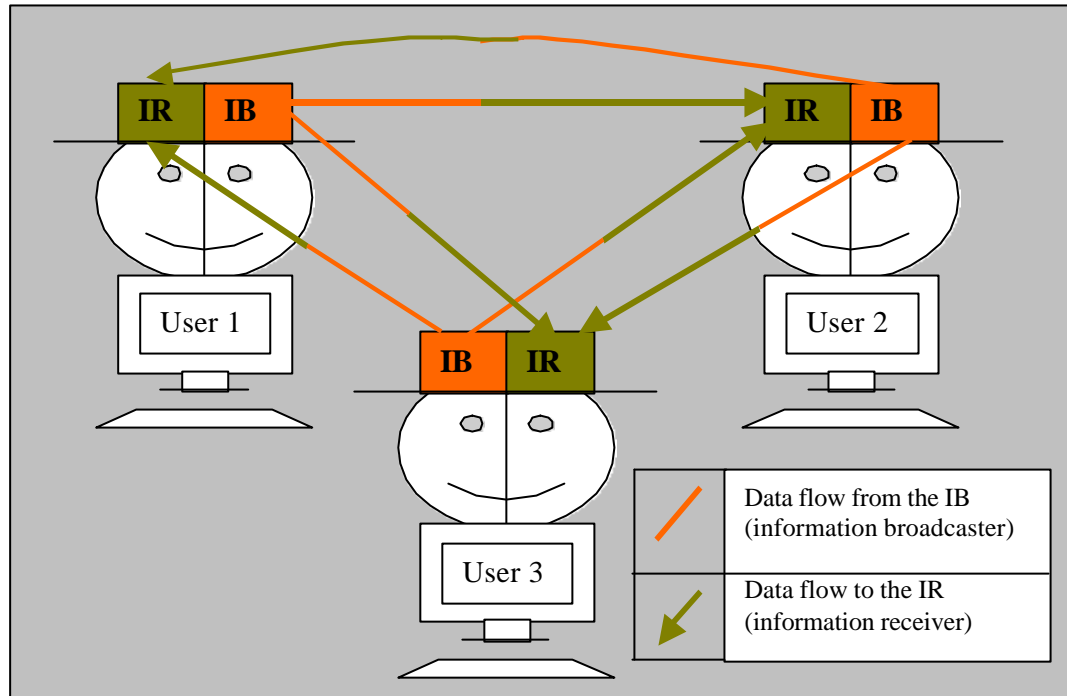


Diagram 8.3: The two user roles of information broadcaster and receiver

It is as a broadcaster that the user takes *privacy risks* and as a *receiver* that the user receives *benefits* and privacy norms are enacted. However, as a receiver the user must have feedback of what privacy behaviours are acceptable to the *information broadcaster* and control over the technology to implement acceptable behaviours. If these are not in place, the likelihood of unintentional invasions of privacy increase (Table 8.3).

<u>Grounded Theory thesis verification</u>
• Previous literature (general): Section 2.3
• Previous literature (HCI): Sub-section 3.3.2
• Study 2: Sub-section 5.2.3.1
• Study 4: Sub-sections 6.1.3.1, 6.1.3.4
• Study 5: Sub-section 7.1.3.1

²⁸ Goffman (1981) talks about this distinction within interactions as that of the speaker and the hearer.

PRIVACY INVASION CYCLE EXAMPLE		
Users' assumptions	User as broadcaster and receiver assumes that real world social norms will effectively protect them from unacceptable behaviour.	
Technology breaches assumptions	Technology isolates the <i>Information Broadcaster</i> (IB) and <i>Receiver</i> (IR) from effectively communicating social norms of acceptable or unacceptable behaviour whilst providing the IB with more control over the data received.	e.g. all of the thesis results have identified unintentional invasions of privacy often due to misunderstanding of what the <i>information broadcaster</i> would perceived as potentially invasive data or behaviours (see Sub-sections 5.2.3.1, 6.1.3.1, 6.1.3.4, 7.1.3.1).
SOLUTION	Provide feedback to the IR of IB's perceptions of the <i>Information Sensitivity</i> and acceptable behaviours, which could help to develop a joint understanding of the data being transmitted.	

Table 8.3: The user distinction and the *privacy invasion cycle*

8.3.1.3 System interaction

Users can vary in their levels of interaction with the system. Videoconference users directly interact with the system whilst conference presenters and some awareness technology users do not. Privacy issues are key in the latter as the user only partakes in the role of *Information Broadcaster* with all the *risks* and no immediate *benefits* to trade-off against those *risks* (Table 8.4)

PRIVACY INVASION CYCLE EXAMPLE		
Users' assumptions	Multimedia communication users may be unaware that they are using the technology or believe their interaction levels are low	
Technology breaches assumptions	Technology advancements makes unobtrusive cameras easy to place and easier to use for zooming, taking a sweeping view etc. This then increases the possibility of breaching users' assumptions of their interaction levels being low. This can occur both intentionally and unintentionally by the technology deployers.	e.g. Departmental common room users' images were broadcast over the Internet without prior awareness by the IB's (see Sub-section 7.1.3.1), multicast conference sessions transmit images of attendee's over the Internet often without prior awareness by the <i>information broadcasters</i> (see Sub-section 6.1.3.1)
SOLUTION	Provide feedback to users of technology usage (audio & video) and interaction levels	

Table 8.4: System interaction levels and the *privacy invasion cycle*

Grounded Theory thesis verification

- **Previous literature (HCI):** Section 3.2
- **Study 4:** Sub-sections 6.1.3.1
- **Study 5:** Sub-section 7.1.3.1, 7.1.3.5

8.3.2 Privacy factors: Information Sensitivity

The privacy factor *Information Sensitivity* relates to the users' perceptions of the data being transmitted and the information received.

8.3.2.1 Information sensitivity judgements

Users make judgements about information sensitivity via a scale of sensitivity. Users' judgements were found to be guided by how personally defining the information was perceived to be and how they perceived others would interpret it (Table 8.5).

Grounded Theory thesis verification

- **Previous literature (general):** Section 2.3 Sub-sections 2.2.2, 2.3.1
- **Previous literature (HCI):** Sub-section 3.2.2
- **Study 1:** Sub-section 5.1.3
- **Study 3:** Sub-section 5.3.2.1
- **Study 5:** Sub-section 7.1.3.2

PRIVACY INVASION CYCLE EXAMPLE		
Users' assumptions	The user (IB) may have a perception of what data is being transmitted and thus how the information regarding them will be perceived.	
Technology breaches assumptions	However, the technology may be distorting the transmitted data. Without feedback to the IB of what the IR is receiving their behaviour may be inappropriate and their assumptions breached.	e.g. camera angles, poor quality data (audio, video), IR zooming in & enlarging IB's image, giving a distorted image of the IB (see Sub-section 5.1.3 & 7.1.3.2)
SOLUTION	<ul style="list-style-type: none"> • Provide feedback to the IB of what the IR is receiving, • Designers & Technology deployers should assess the privacy <i>risk</i> of camera shots or angles • Provide feedback to users of how and where to place cameras for reduced privacy invasion 	

Table 8.5: Users' information perceptions and the *privacy invasion cycle*

8.3.2.2 Public or private situation

The *Information Broadcaster's* perception of how public or private the situation being broadcast is can effect how personally defining the information is (see *Information Receiver*). Certain behaviours may be socially acceptable in private but not in public and visa versa. Misinterpretations of how public a situation is can produce inappropriate behaviour for the situation (Table 8.6).

<u>Grounded Theory thesis verification</u>
<ul style="list-style-type: none"> • Previous literature (general): Sections 2.1, 2.3 and Sub-section 2.1.1 • Previous literature (HCI): Section 3.2 and Sub-sections 3.2.2, 3.4.2 • Study 5: Sub-section 7.1.3.2, 7.1.3.5

PRIVACY INVASION CYCLE EXAMPLE			
Users' assumptions	The user (IB) assumes that the privacy of a real world situation will be replicated virtually.		
Technology breaches assumptions	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%;">Technology can make a private situation public and a public situation private without the user fully understanding the boundaries of the situation.</td> <td style="width: 50%;">e.g. Multicast technology made a real world situation perceived as private or semi-private, public without the users' full awareness of this occurring. Users noted that they would be inappropriately perceived as an exhibitionist for behaving in an unsuitable way for a public situation. (see Sub-sections 7.1.3.2 , 7.1.3.5)</td> </tr> </table>	Technology can make a private situation public and a public situation private without the user fully understanding the boundaries of the situation.	e.g. Multicast technology made a real world situation perceived as private or semi-private, public without the users' full awareness of this occurring. Users noted that they would be inappropriately perceived as an exhibitionist for behaving in an unsuitable way for a public situation. (see Sub-sections 7.1.3.2 , 7.1.3.5)
Technology can make a private situation public and a public situation private without the user fully understanding the boundaries of the situation.	e.g. Multicast technology made a real world situation perceived as private or semi-private, public without the users' full awareness of this occurring. Users noted that they would be inappropriately perceived as an exhibitionist for behaving in an unsuitable way for a public situation. (see Sub-sections 7.1.3.2 , 7.1.3.5)		
SOLUTION	Obtain users' perceptions of the situation. Never assume that your perceptions of a situation are those of the user. What may be clearly public to the designer can be just as clearly private to the user.		

Table 8.6: Users' situation perceptions and the *privacy invasion cycle*

8.3.2.3 Primary and secondary information

Information has two privacy levels within it:

- i) Primary Level²⁹: the actual information being transmitted.
 - ii) Secondary Level: the social-psychological characteristics of the information being transmitted.
- ❖ *Secondary Level* information that can personally define (e.g lazy, emotional, religious) the user in a negative way will increase in sensitivity (Table 8.7).
 - ❖ The *Primary Level* of the information may greatly affect the perceived sensitivity of the *Secondary Level* information, or vice versa.

²⁹ Highly sensitive primary information, which is personally defining, can relate, for example, to the traditional paradigm of *Personal Information*. Here the sensitive nature of the information is immediately apparent e.g medical information, person finance information etc.

- ❖ If multimedia *Secondary Level* information is recorded this increases its sensitivity as the potential to repeatedly review the information is increased.

<u>Grounded Theory thesis verification</u>	
• Previous literature (general):	Sub-sections 2.2.1, 2.2.2, 2.2.4, 2.3.1
• Study 2:	Sub-sections 5.2.2.1, 5.2.3.1
• Study 3:	Sub-section 5.3.2.1
• Study 4:	Sub-sections 6.1.3.1, 6.1.3.3, 6.1.3.4

PRIVACY INVASION CYCLE EXAMPLE		
Users' assumptions	The user (IB) in a videoconferencing discussion has often been found to assume that only the primary level of information relates to potential privacy invasions.	
Technology breaches assumptions	Secondary level information is also relayed which can be distorted by the technology (poor quality data, poor interface design), OR allow the IB to intentionally or unintentionally distort it (the time at which an interaction occurred, who the data was from), invading either the broadcaster or receiver's privacy.	e.g. Technical information (primary level) although apparently innocuous, with poor quality data, could portray negative secondary level information about the IB as inattentive, asleep etc. - see context or interface issues (see Sub-sections 5.2.2.1, 5.2.3.1 & 6.1.3.1, 6.1.3.3, 6.1.3.4)
SOLUTION	<ul style="list-style-type: none"> • Feedback to user of what the IR receives & how accurate that data is. • Provide accurate potential threat feedback when appropriate (e.g to detail increased media use, potential increase in threats, when the session becomes emotive, when potentially embarrassing behaviours occur etc.) 	

Table 8.7: Users' information level perceptions and the *privacy invasion cycle*

8.3.2.4 Trade-offs

- ❖ The perceived degree of *Secondary Level* information being broadcast (and trade-offs) can relate to interactions with the other privacy factors: *Information Receiver, Usage, Context*
- ❖ Increased *Information Sensitivity* levels can be due to the fact that different types of multimedia data increases the amount of *Secondary Level* information being relayed e.g:
 - text textual cues : the way things are presented by the *Information Broadcaster*, abusive language used etc.
 - audio verbal cues : tone of voice, accent.
 - Video visual cues : dress & look of *Information Broadcaster*, mannerisms of the *Information Broadcaster* etc.

However, audio data, in isolation, is perceived as significantly more invasive than visual data, in isolation (see Chapter 7). If a single media is used within an awareness technology a stand-alone audio microphone, would be perceived as significantly more invasive than a stand-alone video camera (without audio).

Grounded Theory thesis verification

- **Study 2:** Sub-sections 5.2.2.1, 5.2.3.1
- **Study 4:** Sub-sections 6.1.3.3, 6.1.3.4

8.3.3 Privacy factors: information receiver³⁰

The privacy factor *Information Receiver* relates to the user's perception of the person who receives and or manipulates their information.

8.3.3.1 Trust

This research has identified that, with regard to privacy, trust is not a linear factor. A highly trusted *Information Receiver* will not automatically be acceptable to receive highly sensitive information.

Grounded Theory thesis verification

- **Previous literature (general):** Sub-sections 2.3.2, 2.4.1
- **Previous literature (HCI):** Sub-section 3.2.1
- **Study 2:** Sub-section 5.2.2.2
- **Study 3:** Sub-sections 5.3.2.2, 5.3.2.3
- **Study 4:** Sub-sections 6.1.3.1, 6.1.3.2
- **Study 5:** Sub-section 7.1.3.2, 7.1.3.6

8.3.3.2 Relationships

If data, that could define the user negatively, is viewed by someone with a close relationship to the user this will make the data more sensitive than if it was viewed by a complete stranger (see Diagram 8.4). We may not mind how someone living thousands of miles away (who we're never going to meet) views our beliefs, our attitudes and us but for a close friend the personal *risks* involved increase ten fold – or more (Table 8.8).

Grounded Theory thesis verification

- **Previous literature (general):** Sub-sections 2.3.2, 2.3.4,
- **Study 2:** Sub-section 5.2.2.2
- **Study 4:** Sub-section 6.1.3.1
- **Study 5:** Sub-section 7.1.3.3

³⁰ When reviewing the users' perception of the information receiver it is the perception of another information receiver NOT their perception of themselves as an information receiver.

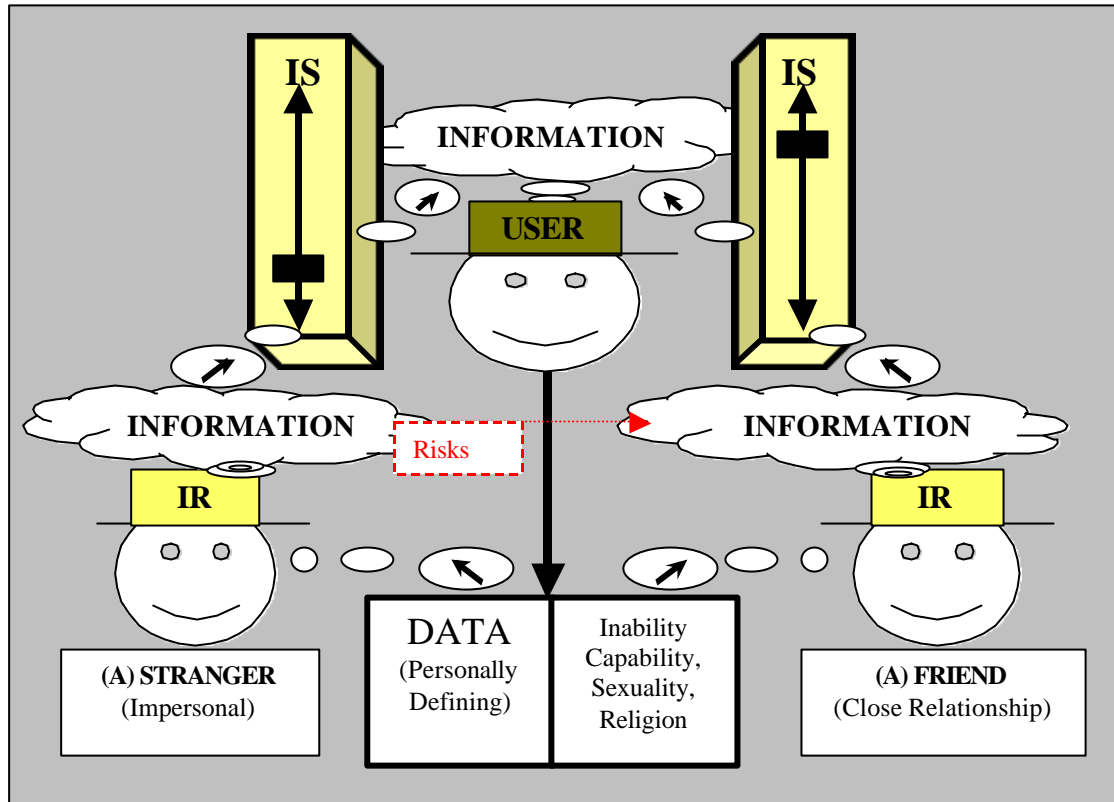


Diagram 8.4: The effect of relationship's on **Information Sensitivity** levels

PRIVACY INVASION CYCLE EXAMPLE		
Users' assumptions	User may assume that multimedia data released to a stranger will not find its way back to friends and colleagues. (close relationships increase data sensitivity)	
Technology breaches assumptions	Technology (trust mechanisms) which automatically determines data released to strangers as low sensitivity information and thus accessible to trusted third parties, with close relationships to the user, breaches these perceptions.	e.g. It may be okay for a stranger to know what we eat and drink but it may be totally unacceptable for a close friend or family to see the same data. The latter's perception can have direct consequences on our interactions (see Sub-section 5.2.2.2, 6.1.3.1, 7.1.3.3)
SOLUTION	Provide feedback on IR's including, clearly, the distance from the IB (physical & organisational). This allows the user to assess <i>privacy risks</i> associated with the interaction. Also provide feedback to the IR of IB's information perceptions & acceptable IR's	

Table 8.8: Users' **Information Receiver** relationship perceptions and the **privacy invasion cycle**

8.3.3.3 Trade-offs: trust

High trust levels in some close relationships *may* be traded-off, at the users' discretion, against increased *privacy risks* allowing more sensitive information to be released.

<u>Grounded Theory thesis verification</u>
<ul style="list-style-type: none"> • Previous literature (general): Sub-sections 2.3.2, 2.3.3, 2.4.3 • Previous literature (HCI): Sub-section 3.2.1, 3.3.1, 3.3.3 • Study 2: Sub-section 5.2.2.2 • Study 4: Sub-section 6.1.3.2

8.3.3.4 Trade-offs: roles

- ❖ A *stranger* viewing data, which can be personally defining, decreases its sensitivity. However, there is always the *risk* of it being released to those (close to the user) who would increase its sensitivity. This is often traded off against the role that the *Information Receiver* plays in the data (e.g. see sub-section 5.2.2.2).
- ❖ Although *close relationships* may increase the sensitivity of the information the role that the *Information Receiver* plays in the data can be traded off against those *risks*. (Table 8.9)

<u>Grounded Theory thesis verification</u>
<ul style="list-style-type: none"> • Previous literature (general): Sub-sections 2.3.2, 2.4.3 • Previous literature (HCI): Sub-section 3.3.3 • Study 2: Sub-section 5.2.2.2 • Study 3: Sub-section 5.3.2.2, 5.3.2.3

PRIVACY INVASION CYCLE EXAMPLE		
Users' assumptions	The IB assumes that the IR is not only trusted but more importantly has an appropriate role in the current and later <i>Information Usage</i> (IR , IU interaction)	
Technology breaches assumptions	Technology or its implementation may relay information to an <i>Information Receiver</i> that although highly trusted does not have an appropriate roles within the data's immediate or later usage.	e.g. An employer viewing a multicast interview would be acceptable because of their role in the <i>Information Usage</i> and the trust ensured by that role & the organisational context. However although the employee may highly trust a close friend (disclosing relationship details not acceptable for the employer to know) they may not be acceptable to view the interview (see Sub-section 5.2.2.2).
SOLUTION	Trust must not be obtained or relayed on a linear level but always in relation to the specific <i>Information Usage</i> .	

Table 8.9: Users' *Information Receiver* role perceptions and the *privacy invasion cycle*

8.3.3.5 Trade-offs: group membership

Users often perceive *Information Receivers* as belonging to specific social groupings, which have roles in the data (Table 8.10). These social groupings can also develop specific interaction styles (e.g colloquial language) that could be misinterpreted by outsiders to the group.

<u>Grounded Theory thesis verification</u>	
•	Previous literature (general): Sub-sections 2.2.3, 2.3.2, 2.4.1, 2.3.4
•	Previous literature (HCI): Sub-section 3.4.2
•	Study 2: Sub-section 5.2.2.2
•	Study 3: Sub-section 5.3.2.3
•	Study 4: Sub-sections 6.1.3.1, 6.1.3.2
•	Study 5: Sub-sections 7.1.3.2, 7.1.3.6

PRIVACY INVASION CYCLE EXAMPLE			
Users' assumptions	The user (IB) assumes that the data will be viewed by within group members. Data perceived as innocuous with low sensitivity when transmitted to within group IR's.		
Technology breaches assumptions	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%;">Technology can increase the sensitivity of the data if transmitted to IR's who are outside the group membership with no acceptable (to the user) role in the data.</td> <td style="width: 50%;">e.g. Multicast sessions were viewed as low in sensitivity when transmitted to within group IR's but highly sensitive for outsiders (without appropriate roles in the data) to view. Technology deployers neglected to realise this factor when transmitting the data to outsiders thus invading users' privacy perceptions (see Sub-section 5.2.2.2, 6.1.1.1, 6.1.3.1, 6.1.3.2).</td> </tr> </table>	Technology can increase the sensitivity of the data if transmitted to IR's who are outside the group membership with no acceptable (to the user) role in the data.	e.g. Multicast sessions were viewed as low in sensitivity when transmitted to within group IR's but highly sensitive for outsiders (without appropriate roles in the data) to view. Technology deployers neglected to realise this factor when transmitting the data to outsiders thus invading users' privacy perceptions (see Sub-section 5.2.2.2, 6.1.1.1, 6.1.3.1, 6.1.3.2).
Technology can increase the sensitivity of the data if transmitted to IR's who are outside the group membership with no acceptable (to the user) role in the data.	e.g. Multicast sessions were viewed as low in sensitivity when transmitted to within group IR's but highly sensitive for outsiders (without appropriate roles in the data) to view. Technology deployers neglected to realise this factor when transmitting the data to outsiders thus invading users' privacy perceptions (see Sub-section 5.2.2.2, 6.1.1.1, 6.1.3.1, 6.1.3.2).		
SOLUTION	Provide clear feedback on who is viewing sessions remotely or who may be viewing recordings in the future - thus relaying to the user potential <i>risks</i> of those outside the community viewing the sessions.		

Table 8.10: Users' *Information Receiver* group membership perceptions and the *privacy invasion cycle*

8.3.4 Privacy factors: Information Usage

The privacy factor *Information Usage* relates to the user's perception of how their information is currently being used or at a later date.

8.3.4.1 Current Information Usage: task³¹

The *task* is a key factor affecting *Information Sensitivity* levels and thus changing trade-offs made. It is important for multimedia designers and those deploying technology to identify if the data is used by the *Information Receiver* for the same task as that perceived by the *information broadcaster*. It is also important for multimedia designers to emphasize to both the *Information Broadcaster* and *Information Receiver* what is acceptable *task usage* for the data.

Grounded Theory thesis verification

- **Previous literature (general):** Section 2.3
- **Previous literature (HCI):** Sub-sections 3.3.3, 3.4.1
- **Study 2:** Sub-section 5.2.2.2
- **Study 3:** Sub-section 5.3.2.4
- **Study 4:** Sub-sections 6.1.3.1

8.3.4.2 Later Information Usage: recording awareness

It is very important that the user has prior knowledge of recording³² as, without this, the user (*Information Broadcaster*) can misjudge appropriate data releases. Later realisation of recording can cause a backlash to potential privacy lapses not accounted for (Table 8.11).

Grounded Theory thesis verification

- **Previous literature (general):** Sub-section 2.1.2
- **Previous literature (HCI):** Sub-sections 3.2.2, 3.3.1, 3.4.1
- **Study 2:** Sub-section 5.2.3.2
- **Study 3:** Sub-section 5.3.2.3
- **Study 4:** Sub-sections 6.1.3.1
- **Study 5:** Sub-section 7.1.3.1

³¹ in all these studies the task of information exchange was reviewed therefore the results should only be considered with these constraints in mind.

³² Re-using information at a later date increases its sensitivity in comparison to mere broadcasting of the information.

PRIVACY INVASION CYCLE EXAMPLE	
Users' assumptions	The user (IB) assumes that the data is only transmitted within context
Technology breaches assumptions	Technology can make recording of multimedia data, without the user's awareness, very easy e.g. "I mean I'd go back and say 'did I say something I shouldn't have said'" (see Sub-section 5.2.3.2), A researcher presenting their findings via videoconferencing, which is recorded and viewed 10 years later, could be viewed as an outdated researcher if the data has not been date stamped. (see Sub-section 6.1.3.1)
SOLUTION	<ul style="list-style-type: none"> User permission to record sessions should be obtained where possible. If this is impractical then feedback to users who are recorded must be provided. Provide context for the data (e.g transmission source, why and when transmitted). Time and date stamp recorded multimedia data so it can be viewed within a temporal context.

Table 8.11: Users' recording perceptions and the *privacy invasion cycle*

8.3.4.3 Later Information Usage: repeated viewing

Recording data increases its sensitivity by giving the *Information Receiver* more control over the data. Pause, rewind and fast forward functions can effectively become an *Information Receiver*'s self-editing tool allowing sections to be missed or repeatedly viewed by an undisclosed number of people. An embarrassing moment can be dismissed but if it is repeated viewed by many more people the invasiveness increases ten fold - or more.

<u>Grounded Theory thesis verification</u>
<ul style="list-style-type: none"> Previous literature (HCI): Section 3.3 Sub-section, 3.3.3 Study 4: Sub-sections 6.1.3.3 Study 5: Sub-section 7.1.3.4

8.3.4.4 Later Information Usage: context

Recording data increases the likelihood of information losing important contextual factors increasing its potential invasiveness (see Table 8.11)

<u>Grounded Theory thesis verification</u>
<ul style="list-style-type: none"> Previous literature (general): Sub-sections 2.1, 2.1.2, 2.3, 2.3.3, 2.4.1 Previous literature (HCI): Sub-sections 3.2.2, 3.4.1 Study 2: Sub-section 5.2.3.2 Study 4: Sub-sections 6.1.3.1, 6.1.3.3 Study 5: Sub-section 7.1.3.5

8.3.4.5 Later Information Usage: editing

Once multimedia data is recorded and later edited there is a higher likelihood that the data out of context will retain secondary information that is personally defining and potentially invasive. The context of re-usage may also affect the sensitivity of the data broadcast (Table 8.12)

<u>Grounded Theory thesis verification</u>	
•	Previous literature (HCI): Sub-sections 3.3.3, 3.4.1
•	Study 4: Sub-sections 6.1.2, 6.1.3.4

PRIVACY INVASION CYCLE EXAMPLE		
Users' assumptions	The user (IB) assumes that they will be informed of data re-use and that it will be kept within its context.	
Technology breaches assumptions	Technology can make the re-use and editing of multimedia data, without the user's awareness, very easy.	e.g. Recorded multicast sessions were edited and re-used, for purposes other than those for which originally recorded, without the IB's permission or awareness (see Sub-sections 6.1.2, 6.1.3.4)
SOLUTION	<ul style="list-style-type: none"> • Feedback to the IR of acceptable (to the IB) information re-uses. • If the data is to be used for another purpose, than those previously flagged to the user, further permission should be obtained. • If data is to be edited (in any way) permission should be obtained from the <i>Information Broadcaster</i>. If this is impractical the privacy implications of editing the data should be considered and edited versions clearly marked with links to original full versions provided. • For highly sensitive information digital watermarking and watercasting should be considered - copying and editing of multimedia data can then be traced. It would be ideal if this action was automated to save the user trawling through data trying to find if their data is on public display somewhere. Again, these actions could help to provide feedback on unacceptable practices in multimedia usage behaviours thus developing acceptable social norms. 	

Table 8.12: Users' re-use perceptions and the *privacy invasion cycle*

8.3.4.6 Trade-offs: risk or benefits

Benefits from the current *Information Usage* may trade off against *risks* from data being released. However, this research has highlighted that, in multimedia communications, users often misinterpret *benefits* and potential *risks*. When data is re-used (out of context) at a later date privacy *risks* are increased especially if the task purpose or *Information Receiver* changes. Changes in later usage may make previous user trade-offs inappropriate.

Grounded Theory thesis verification

- **Study 4:** Sub-sections 6.1.3.1, 6.1.3.2
- **Study 5:** Sub-sections 7.1.3, 7.1.3.1, 7.1.3.2

8.3.5 Privacy model: context

Context refers to the user’s perception of the situation and surroundings within which the multimedia communications have occurred. Further research is required to elaborate on these issues to identify changes in the privacy factors for further contexts.

8.3.5.1 Technology: environments

The technical environment and its interface can affect the degree of feedback and control provided, anonymity perceived and thus privacy perceptions. Inaccurate technology conceptions can increase the likelihood that more high sensitivity information is released than the user wishes (Table 8.13).

Grounded Theory thesis verification

- **Previous literature (HCI):** Sub-sections 3.1.1, 3.1.2, 3.1.3, 3.2.2, 3.3.2
- **Study 2:** Sub-sections 5.2.2.2, 5.2.2.3
- **Study 3:** Sub-section 5.3.2.4
- **Study 4:** Sub-sections 6.1.3.2
- **Study 5:** Sub-section 7.1.3.1

PRIVACY INVASION CYCLE EXAMPLE			
Users’ assumptions	User assumes multimedia communications are conversational (IB,IR two-way interaction) NOT television environments because: 1) participation is interactive or semi-interactive 2) transmission limited to some degree.		
Technology breaches assumptions	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%;">The technology does not make the Conversational Vrs. TV distinction and often technology implementation breaches the user’s assumptions</td> <td style="width: 50%;">e.g. multicast conference sessions assumed to be received by semi-interactive conference viewers was broadcast over a hotel TV network without prior awareness by the <i>Information Broadcasters</i> (see Sub-section 6.1.3.2)</td> </tr> </table>	The technology does not make the Conversational Vrs. TV distinction and often technology implementation breaches the user’s assumptions	e.g. multicast conference sessions assumed to be received by semi-interactive conference viewers was broadcast over a hotel TV network without prior awareness by the <i>Information Broadcasters</i> (see Sub-section 6.1.3.2)
The technology does not make the Conversational Vrs. TV distinction and often technology implementation breaches the user’s assumptions	e.g. multicast conference sessions assumed to be received by semi-interactive conference viewers was broadcast over a hotel TV network without prior awareness by the <i>Information Broadcasters</i> (see Sub-section 6.1.3.2)		
SOLUTION	<ul style="list-style-type: none"> • Assess the privacy implications of using alternative media for distribution purposes • provide feedback to user of distribution & media used for distribution 		

Table 8.13: Users’ environment perceptions and the *privacy invasion cycle*

8.3.5.2 Technology: interface issues

There are numerous interface issues surrounding how interface design can affect user perceptions of what and how much data is released (e.g. Table 8.14).

<u>Grounded Theory thesis verification</u>	
•	Previous literature (general): Sub-sections 2.1.1, 2.4.2, 2.4.3,
•	Previous literature (HCI): Sub-sections 3.2.2, 3.4.1
•	Study 2: Sub-sections 5.2.2.3, 5.2.3.1
•	Study 3: Sub-section 5.3.2.4

PRIVACY INVASION CYCLE EXAMPLE		
Users' assumptions	Users can assume that they have more control over their privacy than they actually have.	
Technology breaches assumptions	Users can develop inaccurate privacy perceptions directly due to poor interface design	e.g. Poor VR interface design failed to clearly illustrate how identifiable users actually were (see Sub-section 5.3.2.4). A user (IB) able to freeze frame within a videoconferencing session portrays an inaccurate picture of their attentiveness or even who is actually receiving the data (see Sub-section 5.2.3.1).
SOLUTION	<ul style="list-style-type: none"> • Provide appropriate feedback & control • Inadequate feedback & control can produce inaccurate assessments of the data being broadcast (thus its <i>Information Sensitivity</i>) • Excessive feedback & control can overload the user with information desensitising them to potential <i>privacy threats</i> and increase unintentional invasions of privacy. 	

Table 8.14: Users' interface perceptions and the *privacy invasion cycle*

8.3.5.3 Technology: presence

The users' perceived *presence* within the technically mediated environment could greatly affect perceived *Information Sensitivity* levels. Videoconferencing environments can produce a sense of disembodiment from the context of interaction (Bellotti, 1997). However, increased perceived distance from the group had positive effects on users' concentration and freedom of expression, free from social norm intimidation. Virtual reality environments amplified users sense of anonymity whilst increasing their implicit sense of presence in the action and context via empathy with the avatar (increasing implicit social norm pressure e.g. embarrassment when walking up to a group of avatars talking – 'should I interrupt?'). Within both environments the user might be tempted to release more data than they would within a face-to-face situation thus increasing potential privacy mismatches.

Grounded Theory thesis verification

- **Previous literature (general):** Sub-section 2.1.1
- **Previous literature (HCI):** Sub-sections 3.2.1, 3.2.2, 3.3.1, 3.3.2,
- **Study 2:** Sub-section 5.2.2.3,
- **Study 3:** Sub-section 5.3.2.4
- **Study 4:** Sub-section 6.1.3.1
- **Study 5:** Sub-section 7.1.3.1

8.3.5.4 *Social groupings*³³: *social groups*

Social groups maintain social norms of acceptable or unacceptable behaviours. Knowing what is acceptable or not acceptable within a specific social group is hindered, within some environments, by poor contextual or social cues. However, some behaviour is considered *private* to the individual (outside social norms) with privacy invasions producing the strongest emotive responses.

Grounded Theory thesis verification

- **Previous literature (general):** Section 2.1, 2.3 & Sub-sections 2.2.4, 2.3.4, 2.4.1, 2.4.2
- **Previous literature (HCI):** Sub-sections 3.2.1, 3.3.1, 3.3.2, 3.4.2
- **Study 2:** Sub-sections 5.2.2.2, 5.2.2.3
- **Study 3:** Sub-section 5.3.2.4
- **Study 5:** Sub-sections 7.1.3, 7.1.3.2

8.3.5.5 *Social groupings: social group outsiders*

During technology mediated interactions, *Information Receivers* from outside the social grouping can be perceived to either inhibit or change collaborative discussions (often misinterpreting transmitted data).

Grounded Theory thesis verification

- **Previous literature (general):** Section 2.1
- **Study 2:** Sub-section 5.2.2.3
- **Study 4:** Sub-section 6.1.2, 6.1.3.2
- **Study 5:** Sub-section 7.1.3.2

³³ See IR for *privacy invasion cycle* examples

8.3.5.6 Organisational culture³⁴: organisational norms

Differences in organisational norms can affect the acceptability of different technology and its implementation. However, a lack of feedback to users and *Information Receiver*'s of acceptable and unacceptable practices within the organisation has been identified on several occasions.

Grounded Theory thesis verification

- **Previous literature (general):** Section 2.3 Sub-sections 2.3.2, 2.3.4, 2.4.1
- **Previous literature (HCI):** Sub-sections 3.2.1, 3.3.3, 3.4.2
- **Study 1:** Sub-section 5.1.4.1
- **Study 2:** Sub-sections 5.2.2.1, 5.2.2.2
- **Study 4:** Sub-section 6.1.3
- **Study 5:** Sub-section 7.1.3.6

8.3.5.7 Organisational culture: trust

The *trust* felt in the organisation will have a direct effect on users' initial perceptions of *privacy risks* associated with the new technologies adopted by the organisation. This means that users' initial lack of privacy fears may be due to a feeling of *trust* in the organisation and not a lack of interest in *privacy risks*. If privacy factors are ignored by the organisation and users' privacy is subsequently invaded users' *trust* in the organisation will decline.

Grounded Theory thesis verification

- **Previous literature (general):** Sub-sections 2.3.3, 2.3.4, 2.4.1,
- **Previous literature (HCI):** Sub-sections 3.3.3, 3.4.2
- **Study 4:** Sub-sections 6.1.3, 6.1.3.2
- **Study 5:** Sub-section 7.1.3.6

8.3.5.8 National and international: cultural norms

These are important in international interactions. However, this research has been restricted to UK and US cultural boundaries therefore the results should only be considered with these constraints in mind.

Grounded Theory thesis verification

- **Previous literature (general):** Sub-section 2.1
- **Previous literature (HCI):** Sub-section 3.4.2
- **Study 2:** Sub-section 5.2.2.2
- **Study 5:** Sub-section 7.1.3.2

³⁴ Further research is required to identify *privacy invasion cycle* examples and solutions for Organisational, National and International context factors.

8.4 MODEL APPLICATION

It must be understood that this *privacy model* is not a “*single integrated model of context and the technology*” (p.574) for, as proposed by Clarke & Cockton (1999) it would be imprudent to assume that it is complete or correct in every detail it does describe. Instead the model seeks to be a guide to help designers collect appropriate privacy related contextual information for the development of their specific multimedia application.

The model should act as a guide to identify potential privacy problems before they occur. These problems can then be researched further and developed into appropriate mechanisms or policies for each specific situation. The factors in this model, however, are not static but change in importance within different contexts. There is, therefore, a need for an account, for designers, of how the model should be applied to specific multimedia communication applications:

1. Represent design and context aspects of the application.
2. Identify privacy sensitive factors that relate to this *privacy model* that may potentially produce privacy invasive actions.
3. Adapt the design or develop appropriate implementation policies.

To understand how the model would work in practice the following actual multimedia communication example is used to highlight, *in a very simplified way*, the application of the model for multimedia designers.

The 1st stage of the evaluation identifies which privacy model factors are applicable for this scenario, what factor interactions occur and how important they are for this scenario. The 2nd stage of the evaluation assesses how users assumptions affect these factors or factor interactions and how the technology breaches these assumptions to produce privacy invasions.

8.4.1 Privacy multimedia communication scenario

A seminar was multicast (same technology as Study 6 and 7) with the speaker giving the presentation from a small London-based office without anyone else present in the room. There were two audiences for the seminar: one local (London) and one remote (Glasgow). Both audience groups sat in seminar rooms and watched the seminar projected onto a large screen.

During the seminar the audiences either heard audio from the presenter or from the video recording whilst the presenter had all the audio channels open. At the end of the seminar a question and answer session occurred during which all of the audio channels were open.

8.4.1.1 Technical Set-up

PowerPoint slides and a video recording, from a previous seminar, were used as part of the seminar. The slides were transmitted as a vic stream and the recording was played out from a VCR through this stream too (i.e. the image was switched from the slides to the clip, and then back again).

All the screens (both audiences and the presenter) displayed 4 tiled windows of images:

1. The London audience
2. The Glasgow audience
3. The presenter
4. The seminar slides / video

The size of the windows displayed to the audiences were:

- | | |
|--------------------------------------------|----------------------------------|
| • Presenter | Common Intermediate Format (CIF) |
| • Glasgow / London remote viewed image | CIF |
| • Glasgow / London viewing their own image | Thumbnail |
| • Slides / video recording | Super CIF |

The presenter saw their image on their desktop screen at window size Quarter CIF whilst the two audiences and the slides / video recording was thumbnail.

8.4.1.2 Participants

The audiences had varying degrees of multimedia communication experience from novice to expert whilst the presenter was experienced in multimedia communications. Although the participants of each audience knew each other they did not know the remote audience or the seminar presenter. Consequently the seminar presenter knew none of the people watching the seminar.

8.4.2 Scenario privacy evaluation: 1st stage

This scenario is evaluated initially for each of the model factors to assess whether the *privacy invasion cycle* could be evoked for some of the participants.

8.4.2.1 User factors

- **Mental models (experience etc.):** Because of the complexity of this scenario users' mental models may have been at odds with what was actually occurring. This could have evoked the *privacy invasion cycle* especially with the novice users who:
 - a. Did not receive enough verbal (e.g briefing, de-briefing) or hard copy information about how the technical process worked.
 - b. Did not have adequate interface (context: interface issues) feedback on how and what the technology transmitted.
- **Information broadcaster or receiver:** There is the potential, in this scenario, for users to have distorted information receiver / broadcaster perceptions that could elicit the *privacy invasion cycle*
- **Direct or indirect system interaction:** Variations in system interaction levels, throughout the seminar, could encourage users to misinterpret their broadcasting roles increasing the likelihood of triggering the *privacy invasion cycle*

8.4.2.2 *Information Sensitivity*

- **Information sensitivity judgements:** Because of the complexities in system interaction levels, for this scenario, there is a potential for users to misinterpret what information is being broadcast (i.e. who is receiving what image, who can hear what) and thus how potentially sensitive the interaction is. This could then activate *privacy invasion cycle* perceptions.
- **Public / private situation:** Although the audiences were in a semi-public seminar the actual seminar situation they attended was local to them. Their images and audio, however, were transmitted to a remote location. This perceptual discrepancy could increase the likelihood of *privacy invasion cycle* misinterpretations. The presenter, in an isolated office, could also misinterpret how public the seminar was.
- **Primary and secondary information:** As images and audio were transmitted to remote viewers from a local group there is an increased likelihood that secondary level information could be misinterpreted thus evoking the *privacy invasion cycle*. Things said and done which are acceptable for a local group could be misinterpreted (with personally damaging secondary level information) by remote outsiders. The presenter being in a secluded location with poor feedback of what the audiences are receiving (i.e. presenter sees small images transmitted but large screen images are watched) may also be more likely to misinterpret audience responses or the degree of secondary level information being transmitted.
- **Trade-offs:** As the privacy model has identified, the degree of media transmitted increases the amount of secondary level information received and thus the potential invasiveness of the information. Users misinterpreting the degree of media being transmitted could trigger *privacy invasion cycle* responses.

8.4.2.3 *Information Receiver*

- **Trust levels:** As already noted the local audience members already knew each other and had established trust levels which may have been at odds with their trust in remote viewers thus potentially prompting *privacy invasion cycle* reactions.
- **Trade-off's (roles, group-membership):** The users may have traded-off privacy against the acceptable trust levels of recipients. However if they are not fully aware of who the receivers are this could trigger *privacy invasion cycle* responses

8.4.2.4 *Information Usage*

- **Current information usage (task):** As participants often take part in seminars, which are not mediated by technology, there is an increased likelihood of incorrect *privacy invasion cycle* assumptions being made about later information usage.
- **Later information usage (recording, editing):** The seminar participants – audience and presenter - were not advised or given feedback (context: interface issues) about whether the seminar was recorded and would be viewed or edited at a later date. A subsequent misunderstanding about the seminar's permanence could, therefore, increase the likelihood of *privacy invasion cycle* perceptions being initiated if data re-use does occur.

8.4.2.5 Context

- **Technology (environments, interface usability):** Poor privacy interface issues interacted with all the other privacy factors to increase the likelihood of inaccurate privacy assumptions being made and thus initiating the *privacy invasion cycle*.
- **Social grouping (social norms, social groups) / Organisational culture (organisational norms, organisational trust):** Differences in location for the two audiences and the presenter could have caused privacy assumptions to occur based on different social and organisational norms thus triggering the *privacy invasion cycle*.

8.4.3 Scenario privacy evaluation: 2nd stage

The privacy model factors and factor interactions are now evaluated to identify potential user assumptions and how the technology could breach these assumptions to produce privacy invasions. Further research is usually required to identify in more detail how important each of these potential invasions are for the user within this specific context (e.g. organisational norms, users initial trust levels).

USER FACTOR : PRIVACY INVASION CYCLE	
Users' assumptions	Low system interaction levels could produce user assumptions that they are only information receivers producing an assumed mental model of the scenario as similar to television or cinema.
Technology breaches assumptions	The technology actually also captures video and audio data and should stimulate a mental model similar to that of the telephone because of its two way communication elements.

INFORMATION SENSITIVITY FACTOR: PRIVACY INVASION CYCLE	
Users' assumptions	<ol style="list-style-type: none"> 1) Audience users could assume that as they can only hear the presenter that everyone else can only hear the presenter. 2) All the users could assume that the information receivers are local (i.e. the remote viewers location was not clearly visible) thus producing a perception of a more private situation with local norms of acceptable language, behaviour etc.. 3) The presenter may assume that little habits and mannerisms they have may not be noticeable as the feedback of their image transmitted is on a small screen. 4) With poor feedback on who is receiving audio transmissions this could produce the assumption that no-one receives this data.
Technology breaches assumptions	<ol style="list-style-type: none"> 1) The presenter, however, can hear both of the audiences 2) The information receivers are actually located across the country and may have different perceptions of acceptable behaviour. 3) The image received, however, is seen on a big screen where their behaviours may look far more dramatic and potentially embarrassing. 4) Audio was, however, received by the presenter throughout the seminar and also by the other audience during the question and answer session.

INFORMATION RECEIVER FACTOR : PRIVACY INVASION CYCLE	
Users' assumptions	User could assume that the images and audio were received only by those visible on the screen.
Technology breaches assumptions	However, the images and audio were also transmitted to recipients not visible on the screen e.g. the seminar technicians.

INFORMATION USAGE FACTOR: PRIVACY INVASION CYCLE	
Users' assumptions	The users could assume that the images and audio were only received live during that seminar.
Technology breaches assumptions	However, the images and audio were actually being recorded and could also be edited at a later date.

CONTEXT FACTOR : PRIVACY INVASION CYCLE	
Users' assumptions	1) Poor interface feedback (e.g. only receiving data, recipients local, data transmitted not sensitive because of small screen feedback etc.) could produce inaccurate user assumptions with regard to what is transmitted. 2) The user could assume that certain unacceptable behaviours would not occur because it is against their social grouping / organisational norms.
Technology breaches assumptions	1) The technology transmits more than is relayed to the user. 2) The recipient norms are those of a different social group / organisation and may be contrary to the broadcasters.

8.4.4 Scenario privacy recommendations

8.4.4.1 Briefing session

System details: A briefing session should be provided detailing how the system works for novice users to establish accurate mental models. They must not be allowed to establish the inaccurate 'television/cinema viewing only' mental model of the system.

Interaction details: The briefing session should establish clearly how public/private the situation is. What may be clearly public to the designer or technology instigator can be just as clearly private to the user (Adams & Sasse, 1999a). It should, therefore, be clearly illustrated to the audiences that although they are attending a seminar (with low system interaction levels) they can still be viewed and heard remotely. They must also understand;

1. when they can be viewed and heard; and
2. who the information receiver is.

Recording details: Clear notification must be given if the seminar is to be recorded stating who will be able to view or edit it at a later date.

8.4.4.2 Interface changes: Information Broadcaster

Data transmission: Present noticeable feedback on what data (i.e. video, audio) a seminar attendee, or presenter, is broadcasting and receiving. Feedback should also be provided to the presenter of how they are being viewed by the audiences, including the image size.

Interaction Feedback: Display obvious feedback of who is receiving the data and when. If the receivers are not part of the interaction they should also be detailed. Also show clearly and in an understandable way ('technically related distances' are not acceptable for novices) the information receiver's current location.

Recording Feedback: Detail noticeable feedback to the information broadcaster of when transmitted data is also being recorded (e.g. a red light going on with the letters REC underneath)

8.4.4.3 *Interface changes: Information Receiver*

Contextual feedback: It is important for information to be kept within its original context. People viewing the session remotely or at a later date must be provided with contextual information (e.g. where transmitted from, why, when - time/date stamp)

Edited data: Edited versions should be clearly marked and links to original versions detailed.

Information handling: Identify if the information receiver is using the information for the same task as that perceived by the information broadcaster. Highlight to both acceptable information usage, e.g. 'for seminar purposes only'

8.4.4.4 *Policy procedures*

Recording permission: Users' permission to record sessions should be obtained where possible. If impractical then feedback to users who are recorded must be provided.

Changed usage: If the information is to be used for another purpose other than those previously detailed to the user a further permission should be obtained.

Editing: Any editing - even minor - to recorded multimedia information should have permission obtained from the user and be carefully reviewed for potential information receiver, usage and context privacy risks

Continued privacy evaluation: Assess the usefulness of the information capture against potential risk of privacy invasion to the user. These assessments can save later costly user trade-offs and rejections of the technology e.g. 'I'm not taking part in or presenting a remote seminar'.

8.5 LOW-LEVEL DESIGN GUIDELINES

For the specific contexts (i.e. studies 1 to 5) that have been reviewed within this thesis the model was used to identify a set of specific design guidelines for similar scenarios (see Table 8.15). These design guidelines can be generalised to similar scenarios. However, it must be remembered that further research is often required to identify the impact of context specific factors (e.g. organisational norms, users trust levels, interface feedback issues). A review by designers of the studies and the model factors will help to determine which aspects are similar and which are not to their specific scenario.

User feedback and control	
Usage awareness, feedback and control:	<ol style="list-style-type: none"> (1) Identify user awareness of multimedia data capture, recording and later usage. (2) Inform users, if unaware of these factors, along with <i>benefits</i> and potential <i>privacy risks</i> so accurate trade-offs can be made. (3) Obtain user permission (where possible) to record. If impractical then provide feedback to users that they are being recorded. (4) If the data is to be edited or used for another purpose than those previously detailed to the user a further permission should be obtained or feedback on re-usage and editing provided.
Feedback on the information receiver	<ol style="list-style-type: none"> (1) Identify who the user believes the <i>Information Receiver</i> to be and how public they believe the situation is. (2) Notify the user immediately if data is transmitted (either currently or at a later date) to people that the user had not envisioned. (3) Provide feedback and control to the user (& IR) on the person(s) to whom the data is transmitted. Include (in an understandable way) the distance the <i>receiver</i> is from the user (physical & organisational) thus allowing accurately assessed interaction <i>privacy risks</i>.
Feedback on data received	Provide feedback to the user on what images & audio the <i>Information Receiver</i> will be intercepting (e.g. degree of distortion)
Users' IR trust appraisal for data release:	Trust mechanisms, which help determine data transmission procedures, should not relate to trust as a linear factor (e.g. highly trusted people allowed access to highly sensitive information). Trust is a highly complex phenomenon which relates to the sensitivity of the information and the <i>Information Receiver's</i> role in that <i>Information Usage</i> as well as the context of usage etc.
Information Receiver feedback	
IR sensitivity feedback	<ol style="list-style-type: none"> (1) Identify what the users' rate the <i>Information Sensitivity</i> levels at. (2) Provide feedback to the IR of users' perceived <i>Information Sensitivity</i> levels + acceptable or unacceptable <i>Information Usage</i> both currently and at a later date.
Data context for IR	<ol style="list-style-type: none"> (1) Provide context for the data (e.g transmission source, why and when transmitted). Time and date stamp recorded multimedia data so it can be viewed within a temporal context. (2) Edited data should be clearly marked with links to original full versions provided. For highly sensitive information digital watermarking and watercasting should be considered - copying and editing of multimedia data can then be traced. It would be ideal if this action was automated to save the user trawling through data trying to find if their data is on public display somewhere.

Table 8.15: Low-level context specific (i.e. studies 1 – 5) design guidelines

Chapter 9: Expert evaluation of the model

As privacy within multimedia communications is an interdisciplinary issue it is important to have input from HCI knowledge and other disciplines. In order to assess how well this HCI model of privacy perception (see Chapter 8) fits with existing knowledge in the other disciplines (i.e. Human Computer Interaction, Multimedia communications, Political Science, Security) the author decided to present it for evaluation to three relevant experts (see Table 9.1). The experts were asked to complete a short review of the model from their own perspective (see Appendix 4 for experts' reviews). The model's rationale and goals were presented to the experts to enable them to effectively evaluate the models success (see Appendix 3 for expert evaluation model package).

NAME	EXPERIENCE or BACKGROUND	WORK SITUATION
Lorrie Faith Cranor	security and privacy expert	Industry (AT&T)
Paul Dourish	technical usability expert	Industry (Xerox)
Michael Muller	participatory design expert	Industry (Lotus Research)

Table 9.1: expert evaluators' of the model

9.1 EXPERT EVALUATION RATIONALE

The model's goal is to aid multimedia designers, implementers, privacy advocates and thus users in two ways:

- 1) As a high-level guide for reviewing the privacy implications of multimedia communication environments and applications from the users perspective. Designers should work through the model factors with regard to their specific context (some factors may be more appropriate to your specific context than others) to identify potential user assumptions being breached by the technology. Then either:
 - i) verify this with further research or;
 - ii) correct the problem with appropriate mechanisms or privacy policies.
- 2) As a low-level user privacy perception input to multimedia communication design and policy making. Designers and technology deployers should review the specific examples of users' privacy assumptions breached by the technology (perceived invasions of privacy) to identify those which relate to their specific context and thus identify and implement the appropriate proposed solutions.

9.2 EXPERT EVALUATION SUMMARY

As this was an interdisciplinary review of the model the reports were presented in an open-ended format. The expert walkthrough reports aimed to help in the model design by identifying:

1. The *completeness* of the model. What aspects were not addressed by the user's perspective and should be addressed - e.g expert privacy advocates perspective (as specifically detailed by the experts).
2. The *versatility* of the model for interpretation by different disciplines. How well understood is the model when translated to another discipline (as specifically detailed by the experts).
3. The *usefulness* of the model. How useful it is to experts from different disciplines (as specifically detailed by the experts and ascertain this from Grounded Theory analysis of the differing perspectives experts adopt).

9.2.1 Expert reviews: models' Positive elements

All of the expert reviews identified that the model fulfilled, to some degree each of the three elements mentioned above.

9.2.1.1 Completeness

It was important to identify if the model was consistent with expert experiences. The findings identified few inconsistencies with expert's experiences with privacy perceptions.

“Overall this model seems pretty consistent with what I have observed.”

One expert's review suggested that the completeness of the model was;

“a model of privacy issues that spans disciplines”

adding that,

“this model, in itself, is an achievement”.

9.2.1.2 Versatility

The expert reviews were also used to identify how well the model and design recommendations could be related to experts within the field. Although there were some model misinterpretations (detailed in Sub-section 9.2.2 and 9.2.3) many of the important model and design elements were understood by experts.

“The survey is broad, and the recommendations are precise and specific, while maintaining generality – a perfect combination. The model of privacy concerns ... is general and promising, and helps us to understand issues in this area.”

“very specific (and well-justified) design tips to reduce risks to privacy in multimedia systems.”

“The model-based recommendations or advice’s are concise and specific. They are written to apply to specific, named work areas, such as user trust, user experience, context, and usage. In (appropriate) contrast with the survey and model, the design recommendations are specific, concrete, and implementable.”

9.2.1.3 Usefulness

It is important to identify the usefulness of the model for experts from different disciplines. All of the experts generally identified the usefulness, to different degrees, of the model for designers either as a tool in privacy protection or in identifying privacy issues.

“I think it could be somewhat useful for someone setting up a multimedia communications system if they really wanted to protect privacy and especially if they already had some background in this issue.”

“I think what you’ve done has the potential to be a really powerful tool. The difficulty with privacy is that people think they understand it.”

“ Overall, as I think you already know, I think this is an important thing to be doing. I’m very much in favour, too, of the way you’re trying to do it, working with field materials and so forth.”

“The combination of model and recommendations are a good-to-excellent example of thoughtful researchers working productively with a complex domain and reducing their conclusions to useful outcomes for practitioners (as well as theorists).”

Finally one reviewer specified three useful aspects of the summary:

- ❖ a useful model of privacy issues;
- ❖ a set of well-argued design advice for HCI professionals;
- ❖ an innovative example of the use of Grounded Theory (an increasingly important approach within HCI).

9.2.2 Expert evaluation 1

Expert 1 identified some limitations with the model design that needed reviewing:

9.2.2.1 Presentation limitations

- Abbreviated IS, IR, and IU were noted as confusing and continual reference to full terms suggested (see Sub-section 9.3.1 for evaluation and revision).
- Further definition of what type of privacy the model relates to was requested – with security experts relating privacy to security of data e.g is it transmitted in encrypted form? (see Sub-section 9.3.1 for evaluation and revision).

9.2.2.2 *Applicability for designers*

- General solutions are suggested as being too vague and detailed examples of how feedback should be provided in a non-intrusive, practical way (“*for some of these I believe you have come up with these examples in some of your papers*”) are asked for. It is suggested that this would be usefully presented with examples (see Sub-section 9.3.1 for evaluation and revision).
- The model is suggested as being overall consistent and useful for “*someone setting up a multimedia communications system if they really wanted to protect privacy and especially if they already had some background in this issue*”. However, the applicability for the non-privacy advocate is questioned with a simpler guideline approach suggested “*5 things you can do to protect user privacy in multimedia communication systems*” with “*more specific examples and perhaps a discussion of trade-offs*” (see Sub-section 9.3.1 for evaluation and revision).

9.2.2.3 *Conceptual coherence: privacy invasion cycle*

- The cycle elements of this high-level story-line are questioned as “*The term cycle implies something that is repeated*” whilst the elements that are repeated were missed by the expert (see Sub-section 9.3.1 for evaluation and revision).

9.2.3 Expert evaluation 2

Expert 2 identified some limitations with the model design that needed reviewing:

9.2.3.1 *Presentation limitations*

- It is suggested that the model presentation was too brief to explore the model details such as supporting material for definitions and factor divisions. “*Social norms, organisational norms, cultural norms... what different work are these doing in the framework*” (see Sub-section 9.3.1 for evaluation and revision) .
- Some assumptions of the model are identified and questioned as not being explained fully “*One (implied) is that there IS a compromise position that can be found between the differing information needs of receivers and broadcasters... which isn’t necessarily the case, I suspect*”. “*Another is that participants are known to each other, in two ways; first, that IBs know that there ARE IRs, and second that they know WHO they are, so that they can have a position on their levels of trust. I wondered how this covered cases of unexpected surreptitious or anonymous monitoring*” (see Sub-section 9.3.1 for evaluation and revision).

9.2.3.2 *Applicability for designers*

- The specific solutions and recommendations were noted as not precise enough: “*provide feedback to users*”, “*provide context*” or “*obtain users’ perceptions.*” With, again, feedback required on how these recommendations were derived from the field investigation (see Sub-section 9.3.1 for evaluation and revision).

- A design and deployment consideration is suggested as a problem with the model as it is currently presented. The model is “*oriented towards bespoke development, but much harder to apply to generic or shrink-wrapped software, or situations in which development and deployment are separated*” (see Sub-section 9.3.2 for evaluation and revision).

9.2.3.3 Conceptual coherence: data-information

- The conceptual coherence of the distinction between data and information is queried. It is argued that the model deals with information from the perspective of the *Information Broadcaster* but the IB cannot broadcast information only data “*since information is formed by the interpretation of the receiver*” (see Sub-section 9.3.2 for evaluation and revision)
- A suggestion is made that more emphasis on the data-information issue is required. Further distinction is noted as being required as it is suggested, “*that accumulation of data provides for information which is more than simply the interpretation of the individual data items. The fact that I was not in my office at 9am this morning is relatively meaningless, but the fact that I’m NEVER in my office at 9am might convey more. So items of information do not live in a one to one correspondence with items of data, and the nature of that relationship needs to be better elaborated*” (see Sub-section 9.3.2 for evaluation and revision).

9.2.3.4 Conceptual coherence: user perceptions

- It was suggested that the conceptual coherence of perception is unclear. It is argued, incorrectly, that the model suggests privacy invasions occur through mismatches between “*user’s perceptions and the actual information collected*”. However, this is not a perception, since they have not realised that the information has been collected. It is suggested that the connection between privacy “*invasion*” and a perception or recognition of that invasion has not been clearly stated (see Sub-section 9.3.1 for evaluation and revision).
- It is argued that privacy invasion depends on “*the USE to which the information is put, rather than the information itself*” (see Sub-section 9.3.1 for evaluation and revision).

9.2.4 Expert evaluation 3

The third evaluation only identified problems with the presentation of the model and subsequent design recommendations:

9.2.4.1 Presentation limitations

- It is argued that the relationship between the model and the “*derivative specialisation of it*” in the *privacy invasion cycle* is not explained adequately (see Sub-section 9.3.1 for evaluation and revision).
- It is suggested that “*the applicability of the model to the design recommendations ... may not be clear to some readers*” (see Sub-section 9.3.1 for evaluation and revision).

- Finally the expert notes that “*the innovative (to HCI) use of Grounded Theory*” is not explained in enough detail. “*Some readers whose experience with Grounded Theory is limited to HCI publications (mostly Star and Bowker) may not understand that the authors have made use of another, equally appropriate methodology based on Grounded Theory*” (see Sub-section 9.3.1 for evaluation and revision).

9.3 REVIEW OF THE MODEL

An evaluation of the model by the experts has identified 2 main areas where there are possible problems and potential for advancing the model.

1. As the model is so extensive, a summary of the model was sent to experts for review. Many of the limitations, noted by the experts, are due to the restricted space for explanation. Limited space and inadequate presentation of the ideas resulted in the experts misinterpreting some of the concepts. This thesis presents all of the extra information that the experts noted that they required and which may have fully explained the complex concepts inadequately presented in the model summary.
2. The experts highlighted various areas where the model should be expanded upon and thus where further research is required.

9.3.1 Summary limitations and thesis solutions

Expert 1 noted that the summary abbreviations were too difficult to keep in mind. However, this thesis:

- Extensively reviews the abbreviated concepts of *Information Sensitivity* (IS), *Information Receiver* (IR) and *Information Usage* (IU) so that the reader should not have this problem.
- This thesis also fully explains the type of privacy that is under review (users’ perceptions of privacy) and distinguishes it from security or privacy advocates notions of privacy (see Chapter 2).

All of the experts noted that the model definitions, relationships and recommendations required justification through the founding research. Limited space in the summary, submitted to the experts, did not allow for a justification of the model, explanation of the relationships between different model aspects and an elaboration on the use of Grounded Theory for this research approach.

- This thesis presents all the research on which the model is founded, how the model is derived from that research, how model aspects relate together and a detailed explanation of Grounded Theory as a HCI research methodology (see Chapter 4).
- Finally this thesis presents the application of the model for designers (see Section 8.4) and a low-level context specific set of privacy guideline (see Section 8.5) as suggested by one of the experts. Although it must be understood that designers relying solely on a *quick-fix* 10-point

guide approach would deny the complexity of the phenomenon rendering it incomplete and inappropriate (Clarke & Cockton, 1999).

The experts misinterpreted aspects of the model due to the limited presentation of concepts in the model summary submitted to them:

- It was stated by one of the experts that the model assumed that:

“... participants are known to each other, in two ways; first, that IBs know that there ARE IRs, and second that they know WHO they are, so that they can have a position on their levels of trust. I wondered how this covered cases of unexpected surreptitious or anonymous monitoring.”

However the model does not assume this and on the contrary highlights the importance of the users' awareness of the *Information Receiver*. A lack of *Information Receiver* awareness was identified in the research as a potential cause of privacy invasions. These findings were highlighted by study 4 (Chapter 6) and 5 (Chapter 7) which noted the importance of within group *Information Receiver's* and awareness of data transmission (system immersion levels). The *privacy model* details the relationship between these findings and the *privacy invasion cycle* in Table 8.5 and 8.10.

- It was assumed that for the *privacy invasion cycle* to be a cycle that once trust has decreased it must increase again for the cycle to be repeated. However, the cycle represents an ever-decreasing cycle (a spiral) whereby trust is lowered each time through the cycle until the cycle is broken. Further research is required to identify if this cycle can be effectively broken and how this can be done so that trust can be increased in a contrasting ever-increasing cycle.
- Again one expert misinterpreted the model and the concept of user's perceptions. The expert stated that the model suggested

“privacy invasions occur through mismatches between user's perceptions and the actual information collected and this is not a perception”

However the model states that privacy invasions occur between users' perceptions and the *realisation* that these are inaccurate because of the actual information collected. This *realisation* is again the user's perception of the situation and can similarly be their misconception of the situation (e.g they realise its worse than it actually is – increasing their perceptions of privacy invasions).

- An expert highlighted that they believed that privacy invasion was only due to usage:

“the USE to which the information is put, rather than the information itself”

However the results from study 4 and 5 (see Chapters 6 and 7) highlight that simply transmitting data:

- i) to those considered as outsiders or;
- ii) from situations considered as private;

can be an invasion of privacy without the information being used for any particular invasive purposes. Again it should be noted that this research has identified that privacy invasions can occur unintentionally and without malice.

- It is argued by one of the experts that they do not believe that a compromise between the differing information needs of *receivers* and *broadcasters* is possible. However this research (study 2; Chapter 5 and study 4; Chapter 6) shows that within the specific domain of multimedia communications that, as long as the *information broadcaster* fully understands the *privacy risks* undertaken in an interaction and trades these off against potential *benefits* then, a compromise can be achieved.

9.3.2 Further research

The experts identified several areas where the model could be expanded upon to make it more applicable for designers.

- Further research is required to make the model more applicable to generic or shrink-wrapped software as well as situations where development and deployment are separated.
- There is also further research required to evaluate the data-information distinction in more detail with respect to privacy invasion. Expert 2 suggested that it is only the *Information Receiver* who interprets the data as information. However research has identified that the scenario is far more complex than this. It is suspected that the *Information Broadcaster* interprets the data as information to assess its sensitivity before broadcasting it. They also review how the *Information Receiver* will perceive that data as information to assess its sensitivity. How the *Information Broadcaster* interprets the data, as information is vital to the model and miscalculated interpretations of the data's sensitivity as information is a major cause of the *privacy invasion cycle*. It is also suggested, by expert 2, that the more data intercepted the more invasive the information:

“The fact that I was not in my office at 9am this morning is relatively meaningless, but the fact that I’m NEVER in my office at 9am might convey more”.

However, the research in this thesis would imply that the distinction is even more complex than this expert's argument that 'more data produces a more invasive situation'. Sometimes less data can be more invasive since it can result in a lack of context for the data when it is interpreted (or

misinterpreted) as information. For example, a view of an employee dancing on the Table one morning could produce the misinterpretation that they are odd unless the mouse on the floor and the normal behaviour on other mornings are seen.

9.4 CHAPTER SUMMARY

Three relevant experts from different disciplines were asked to evaluate the model for its *completeness*, *versatility* and *usefulness*. With regard to completeness there were only a few inconsistencies identified between the model and the expert's own experiences. The model is considered versatile, as the experts understood most of the important model and design elements. Finally all of the experts identified the usefulness, to different degrees, of the model for designers either as a tool in privacy protection or in identifying privacy issues.

There were three main problems, however, identified in relation to the model:

1. The summary of the model presented to the experts had its limitations. The summary was too brief and complex and thus many aspects required further explanation and verification.
2. It was noted by one expert that the model was too vague for non-privacy experts to apply. It was suggested that there is a need for a specific recommendations.
3. Further explanation for *privacy invasion cycle* and user perceptions is also recommended.

This thesis has sought to correct these problems with three solutions:

1. This thesis presents all of the extra information that the experts noted that they required and which may have fully explained the complex concepts inadequately presented in the model summary.
2. The model has been expanded upon to further explain complex concepts whilst guidance on its application (see Section 8.4) for designers and low-level context specific recommendations (see Section 8.5) have been provided.
3. Finally the experts identified various areas where the model should be expanded upon and thus where further research is required. These and other areas of further research are detailed in the next Chapter.

Chapter 10: Conclusions

It has been argued that there are many inalienable privacy rights and that privacy experts have a better understanding, than users, of potential privacy risks (Davies, 1997; Bennett, 1997). However, privacy is a socially determined phenomenon that relies on our perception of it. Users' perceptions of privacy are especially important within social interactions since the information imparted is entrenched in our social lives and communication relates to socially determined notions of the individual within society (Goffman, 1969; Agre, 1997). This thesis has, therefore, sought to provide the HCI knowledge base with research and findings into users' perceptions of privacy in multimedia communications (see Section 1.5). More specifically, a model of what guides users' perceptions and a theory of the processes behind privacy invasions was sought. These can help to develop multimedia applications that are acceptable to users, so they are not rejected because of perceived privacy invasions.

This thesis sought to initially focus this research and thus the model upon relevant knowledge in HCI and related disciplines. However, insufficient empirical research has been conducted into users' privacy perceptions. Existing interdisciplinary privacy knowledge (see Chapter 2), although providing some insights does not relate to HCI knowledge on multimedia communications or translate into knowledge useful for designers. In contrast current HCI privacy knowledge (see Chapter 3) is either anecdotal or too application specific to be applicable for designers working within different contexts.

This thesis has developed a descriptive model of users' perceptions of privacy in multimedia communications providing testable theories and guidelines for application designers. This Chapter summarises how the model contributes to the HCI substantive knowledge base and assesses the suitability of methods used to conduct this research for other complex phenomena within HCI.

10.1 SUBSTANTIVE CONTRIBUTIONS

The findings from this thesis have substantively informed the HCI knowledge base in three major ways. Firstly a model of users' perceptions has been constructed, from the empirical findings, with a high level story line identifying the main processes involved in perceived privacy invasions. This model informs the HCI substantive knowledge base with a detailed description of privacy factor relationships (from the user's perspective). Secondly results of the empirical studies have added more specific multimedia privacy guidelines to the knowledge base. Finally the thesis has identified that current approaches to privacy are too limited for the complex nature of multimedia data and associated perceptual processes. Further research is required to extend and integrate the knowledge already accumulated.

10.1. 1 Model findings

Privacy invasion cycle: The research has identified that a descriptive cycle of processes (see Diagram 8.1) is associated with the *privacy model*. Perceived invasive behaviour has been established as related to the mismatch between users' perceptions of *privacy risks* and their *realization* of actual *privacy risks*. A critical boundary has been identified in users' privacy perceptions which, when violated, produces negative emotive responses from users and a rejection of technology.

Model: An explanatory model of the user's perspective of privacy in multimedia environments has been developed. Apart from user role distinctions (see *Information Broadcaster* Sub-section 8.3.1.2) the model (Diagram 8.2) has identified three factors (*Information Sensitivity, Receiver & Usage*), and interactions between them, that are key to users' perceptions of privacy. Users' perception of *Information Sensitivity*, with degrees of sensitivity, details an alternative privacy perspective to previous data-centric approaches. Users' perceptions of the *Information Receiver* identify a range of associated privacy issues including *trust* based on *relationships* and *information roles*. Finally users' *Information Usage* perceptions are presented both during transmission and on later usages. Key privacy *context* issues, which occur within multimedia communications, are also presented in the model. The model helps to determine which information users' regard as private, from whom, and in which context. The model also accounts for *trade-offs* that users make, which render some *privacy risks* acceptable and when these are reliant on *trust*. The model can assist designers and organizations utilizing multimedia communications to assess privacy implications, and assess the acceptable use of the technology.

10.1. 2 Specific guidelines

The results from the studies have also produced a set of low-level design guidelines, related to the specific contexts researched, which will increase computer privacy in multimedia communications (see Sections 8.4 and 8.5). These guidelines will aid designers and policy developers in developing appropriate control and feedback mechanisms and policies in a non-intrusive practical way. The guidelines will also assist organisations with privacy sensitive deployment of multimedia communications. However, further research is needed to expand these guidelines e.g. evaluation of the model on a number of designs and deployments. It must be understood that designers relying solely on *quick-fix* guidelines to fit all scenarios would deny the complexity of the phenomenon (Clarke & Cockton, 1999).

10.1. 3 Privacy approaches

This research has identified that previous approaches to privacy protection are not addressing many important issues within multimedia communications. The two main limitations to previous privacy approaches are:

1. Many multimedia invasions of privacy are not intentional or malicious; rather, designers have failed to anticipate how data could be used, by whom, and how this might affect users.
2. The *Personal Information* approach to privacy is not appropriate for multimedia data since most multimedia data affords identification without being highly sensitive whilst some non-identifiable data can be invasive.

The research detailed in this thesis has also revealed the importance for privacy within multimedia communications of:

- The complexity of information perceptions. A purely data-centric approach to privacy ignores the complex privacy implications of users' data, context and information perceptions.
- Sensitivity levels within information. Understanding interactions between differing sensitivity levels and other factors can help to identify potential privacy trade-off's increasing the acceptability of new multimedia technologies.
- The distinction within the user between the information broadcaster and receiver. Identifying the user role within an interaction can help specify whether specific multimedia communication scenarios are likely to incur higher privacy risks which must be reviewed in more detail.

10.2 METHODOLOGICAL CONTRIBUTIONS

This research required a methodological approach that would aid in the development of a *privacy model* and guidelines with all the relevant issues integrated at all levels of abstraction. The methodological approach was required to identify the problems actual complexity along with relevant contributory issues. Whether it was application specific, organisationally or socially bound, appropriate solutions to problems were sought.

All of the empirical studies, in this thesis, demonstrated that by using the Grounded Theory approach and analysis methods it is possible to identify previously concealed issues, which are pivotal to the relationships uncovered. A methodological contribution of this thesis has been to identify four specific ways in which Grounded Theory can be used to further the accumulation of HCI knowledge for similarly complex phenomena.

10.2.1 Lack of previous research

The thesis research was initially hampered by a lack of previous research, although this situation is not uncommon within the field of HCI, where most issues, due to the nature of computers, are novel and original. This meant that an exploratory type of research was required to detail an accurate description of the phenomenon. However, traditional experimental methods do not work well for this kind of investigation. In contrast, Grounded Theory's ability to loosely focus research and identify theories through later analysis is ideal for this type of exploratory research (Strauss & Corbin, 1990).

10.2. 2 Limitations of previous research

The existing HCI research on privacy did not have a strong empirical basis and lack generalisability (e.g. anecdotal, application specific). Again, the flexibility of Grounded Theory proved advantageous for this research, not only to review previous models but also to compare them with a focused reappraisal of the field. The literature evaluation conducted by this thesis enabled an extraction of what was relevant from previous research whilst providing the data to discard inappropriate theories (e.g. *Personal Information*: see Sub-section 2.2.2, *control and feedback approach*: see Sub-section 3.4.1 – also see Grounded Theory summaries showing progression of model). Being an interdisciplinary field, HCI can obtain an abundance of knowledge from related disciplines but the relevance and application potential of that knowledge has to be assessed and integrated in the HCI knowledge base where appropriate (Sasse, 1997). Grounded Theory was found, for this research, to be able to comply with these requirements and yield a structured hierarchical framework which can not only be used to provide guidance to designers etc., but also provide the starting point for the development of explanatory HCI theories.

10.2. 3 Complex phenomena

The social psychological nature of users' privacy perceptions meant that an elaborate interweaving of complex issues were reviewed in the studies. The ever-changing nature of the phenomenon through different situations, users and temporal contexts brought additional challenges to the research. Grounded Theory's powerful nature when dealing with complex yet vague phenomena made it ideal for this research topic. The development of a detailed framework dealing with factors at differing levels of aggregation addressed the complexity of interweaving issues, whilst the coding processes retained the complexity of interactions affected by differing factors and over time.

10.2. 4 Integration of discipline knowledge

As this research has shown, Grounded Theory can be used to adopt and adapt knowledge from various other disciplines whether they are of a quantitative or qualitative nature. All of the studies reviewed previous research and integrated relevant previous findings into their investigation. This means that findings from other disciplines need not be abandoned for a specific HCI approach but an over-arching analysis of findings can be used to formulate a general HCI substantive knowledge base.

Ultimately this thesis has identified the need for accurate research into relevant HCI issues whilst reviewing existent interdisciplinary knowledge bases in order to build an HCI unified knowledge base with applicable findings for designing usable computer systems. Grounded Theory provides the flexible yet structured approach required for analysing some of the complex, ever changing issues of HCI. It must be added that although Grounded Theory provides the flexibility and power to cope with

the complex multi-disciplinary nature of HCI there is also a question of maintaining adequate quality in the research to retain its validity.

Henwood & Pidgeon (1992) suggest that research is ultimately evaluated in terms of its persuasiveness and ability to inspire. Grounded Theory produces results that are represented at diverse levels of abstraction but that nevertheless fit the data well, providing persuasive, relevant theories. It could be argued that it is this factor that is producing an increase in the methodology's usage across domains (Browning et al., 1995; Clegg et al., 1996) increasing its usefulness in tying together research from multiple domains. Ultimately, a methodological faith or belief should not restrict research. It should rely on questioning and a suspended disbelief. It would be limiting research to adhere religiously to a positivistic or naturalistic paradigm dispelling the *benefits* of one to acknowledge the other. The paradigm non-specific, multidisciplinary abilities of Grounded Theory highlight its ideal qualities for dealing with complex issues within HCI.

10.3 CRITICAL REVIEW OF THE THESIS

There are three major arguments that can be levelled against the research presented in this thesis:

- 1) That the focus of the research is too narrow reducing its validity (see 10.3.1)
- 2) That the findings are only descriptive limiting their generalisation and their integration into the HCI knowledge base. (see 10.3.2)
- 3) That the model is too complex to be applicable for designers (see 10.3.3)

These criticisms relate to the scope of the research, the methodological approach to the research and the resultant findings. Each of these arguments are presented in the next three Sections and reviewed in the light of the thesis contribution aims (see Section 1.5):

1. Providing a fuller understanding of users' perceptions of privacy within multimedia communications.
2. A detailed account of specific privacy invasions and potential solutions within various multimedia environments.
3. The development of a model and theory which will aid in appropriate privacy mechanism, policy design and implementation.
4. The identification of areas for further privacy research within multimedia communications.

10.3.1 Thesis specificity

It may appear that within this thesis a very narrow scope has been taken to privacy i.e.

- 1) Users' privacy perceptions not the data, legal implications, technical possibilities or actualities.

- 2) Within communications rather than database management or ecommerce (although communications does relate to this field).
- 3) Multimedia communications rather than telephone or email communications. Specifically isolating the thesis to applications such as videoconferencing, virtual reality and multicast conferences.

This focused scope means that the implications of the research are limited to a large degree to this domain. However, as the privacy field and relating factors is so complex these restrictions were required for a comprehensive, empirical analysis of the issues to be successfully undertaken. Although a specific scope has been taken the expert evaluation (see Sub-section 9.2.1) highlights the usefulness of these findings both in:

- 1) presenting more evidence of specific occurrences of privacy invasions with potential solutions and;
- 2) increasing our understanding of users' perceptions of privacy in multimedia communications.

Both of these useful introductions to the HCI knowledge base have fulfilled some of the thesis' aims as detailed above.

10.3.2 Thesis findings only descriptive?

This research has produced a theoretical model with explanatory theories. Strauss and Crobin (1990) argue that their theory building places interpretations on the data via 'statements of relationship' rather than merely organising the data according to themes as many descriptive methods do. It could be argued, however, that this thesis is based too much on qualitative research with not enough quantitative findings to substantiate the results thereby increasing their generalisation to other scenarios for designers. However, as previously pointed out (see Chapters 2 & 3), there is no detailed empirical analysis of users' perceptions within multimedia communications to base any quantitative research on. Without prior findings any quantitative research questions would restrict and pre-define privacy thus confounding the results. The research presented in this thesis, however, firstly does not pre-define the phenomena and secondly, using Grounded Theory, takes a scientific structured approach to the collection and analysis of the data thus increasing its generalisability. One of the expert evaluations (see Sub-section 9.2.1 and Appendix 4) specifically emphasised that HCI as a discipline can learn a great deal from the Grounded Theory approach taken throughout this research. The findings from this thesis can now be used, in further privacy research, to elaborate on the model, qualifying the theories for specific environments and within specific fields. This fulfils the fourth aim of this thesis to highlight areas where further privacy research is required.

10.3.3 Thesis complexity

A major problem with the concepts within the model and theories is their complexity, which complicates their dissemination in an effective manner. However, a simplification of the model and its theories can lose the full complexity of the concepts and thus increase the likelihood of their

misinterpretation. This argument can be substantiated by the expert walkthrough where the experts were found on several occasions to misunderstand the model and concepts through the restricted presentation of the model (see Appendix 3) without research findings to explain the concepts further. Ultimately, however, it must be realised that privacy is a very complex, socially determined phenomenon that cannot be simplistically and accurately presented. However, one of the experts evaluating this model noted that

“The combination of model and recommendations are a good-to-excellent example of thoughtful researchers working productively with a complex domain and reducing their conclusions to useful outcomes for practitioners (as well as theorists).”

This research has thus fulfilled several of the thesis aims (as detailed in Section 10.3) by identifying the major privacy concepts within this field so that direction can be given to designers in supporting specific aspects of privacy and further research. A further development of the model has also been placed in the thesis (see Section 8.4), which highlights the contextual elements of the model, and how designers can apply it for specific scenarios.

10.4 HIGH LEVEL IMPLICATIONS

Most of this thesis research into privacy perceptions has highlighted the limitations of current privacy approaches for multimedia communications. The concept of *Personal Information* is employed by many as an assessment of users' potential worries regarding data that is identifiable. However, within multimedia communications, most data is identifiable making it impracticable to treat as *Personal Information*. Conversely, some multimedia data is individually anonymous and yet can be either personally invasive or reflect badly on the individual's privacy, via social grouping privacy invasion. The concept of *Personal Information* relates to the protection of the individual whilst this research has identified that users often associate this socially determined phenomenon as strongly linked to social group norms. Finally one of the complexities highlighted by this research is that privacy perceptions and misconceptions are strongly influenced by the technology mediated environment used for communication. All of the high-level implications from this research are reviewed in the next three Sections.

10.4.1 Personal or not Personal Information divide

Many contributions to the privacy debate often make a simple binary *private - not private* distinction, by devising privacy mechanisms for either all data or just *Personal Information* without clearly defining what this term means to the user. Making this limited personal or not *Personal Information* distinction is the cause of many potential privacy problems. Organisations often assume that a user providing so called, *Personal Information* for accepted organisational practices (e.g providing a service) accepts that this can be used in any way that fits within these parameters. As multimedia data is identifiable within the current privacy paradigm definitions, it must be considered *Personal*

Information. This therefore means that a user's acceptance of its usage often produces organisational acceptance that they may use the data in most ways that they feel fit within the original parameters for acceptability. However, this again makes the mistake of assuming that the data remains at the same degree of sensitivity regardless of slight changes in its usage.

The problem with traditional privacy approaches is not only limited to impracticability of treating all multimedia data as *Personal Information*. The traditional perspective also produces the misguided concept that data which is not personally identifiable (thus anonymous) protects a user's privacy. However, some multimedia environments allow for complete anonymity and yet still produce a perception of privacy invasion. Imagine a situation where a woman goes into a room full of strangers. Everyone seems polite and normal except one person who keeps standing very close to her, often right in front of her, constantly staring at her. Every time she moves around or even out of the room this person follows her. Whenever she starts up a conversation with this person they ignore her but appear to be listening intently when she has a conversation with anyone else. This would appear to be anti-social behaviour and the woman would be justified in feeling this was invasive behaviour. Now imagine that this situation is within a virtual environment where anonymous avatars (graphical representations of the user e.g. cartoon characters) represent everyone. Would the woman feel less invaded or more so? According to the current privacy policy paradigm the woman has not been personally identified and yet she noted these behaviours as invasive. This situation actually occurred and a later investigation proved that these were neither intentional nor malicious anti-social behaviours but totally interface related (see Sub-section 10.4.3).

10.4.2 Social grouping privacy

How we are identified relates very strongly to which context we are identified within. Some social psychologists make the distinction between the personal and the social identity (Auoustinos & Walker, 1995; Tajfel, 1981) where the former relates to characteristics that are strictly individual and the latter to an individual's position within a social group. Within the traditional computer privacy paradigm *Personal Information* relates to both data about an individual (our name etc.) and their social groupings (our ethnic background, political and religious convictions, area in which we live). This highlights the importance of the individual's place within society. However, it could be argued that the social grouping itself has its own identity, which relates³⁵ to the individual. This would mean that although an individual is anonymous if the social grouping is identified the individual is indirectly identified. Within Britain a recent advertising campaign demonstrated this problem when its advertisements detailed a specific street (a social grouping) as containing individuals (not identified) who were breaking the law (i.e. not having a TV licence). People within that street, who were not breaking the law, reacted very negatively to this portrayal to the world of negative details about their street.

³⁵ According to Wacks' (1989) definition of *Personal Information* if the information relates to the individual it could be *Personal Information*. The information, however, may not relate directly but indirectly via a social grouping.

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.

10.4.3 Technologies distorting privacy perceptions

Ascertaining users' privacy perceptions within multimedia communications is a vital step towards developing more acceptable systems. When reviewing users' perceptions it is important to understand how they are constructed. Mental models have been identified as important in enabling us to interact effectively in social situations as well as to adapt to new situations. Our models are based on social and physical cues from our environment as well as our assumptions, based on previous knowledge and experiences (Johnson-Laird, 1983). When environments replicate the real world virtually, they allow users a quicker less stressful entrance to the virtual world. However, if this virtual world is based on limited or inaccurate social and physical cues the users are likely to have inaccurate mental models and be basing their interaction on the wrong assumptions. Some technically mediated environments have been identified as the cause of dissociation and disembodiment from the user actions and the interaction (Bellotti & Sellen, 1993). A lack of facial and body cues, which we take for granted in real world situations, can produce an even more isolating and inhibiting situation for a user. Some researchers have realized the importance of body cues and gestures within these environments and are seeking to replicate them (Rime & Schiaratura, 1991; Marsh, 1998).

As mentioned in Sub-section 2.1.1, technology mediated interactions often lack social, physical and context cues which are required by users to judge accurately the situation and to adapt their behaviour accordingly. This argument is corroborated by my research findings, which highlights user's isolation and disorientation within these environments. Study one identified that when users' feel isolated from social cues they resort to physical cues in the world around them. Respondents not aware of the information's sensitivity or potential security *rISKS* responded instead to their physical environment (*'Well it's hard to get into this building so we must be relatively safe here'*). These findings have serious privacy implications when it is considered that many Internet users communicate from their home - a great source of perceived physical security from privacy invasion.

An individual's failure to identify accurately a situation as private can have devastating consequences. In study five we identified distorted perceptions of the common room situation. Those being observed had different control and feedback from those observing the situation. The observers' increased *control* of the technology distorted their perception of the *place* being observed from those within the situation. In order that users assess a technology-mediated situation accurately they all require adequate feedback and control mechanisms (Bellotti, 1997). Once users' experience a lack of control and respond emotively, a total rejection of the application and all similar technology is the likely

consequence. In this study, those who felt the most discomfort subsequently rejected transmission of any audio and video data under any circumstances.

The importance of feedback to the *Information Receiver* is as important as it is to the user when developing social norms for acceptable behaviours within these environments. The woman in the previously mentioned invasive virtual environment scenario (see Sub-section 10.4.3) assumed the other person's invasive behaviours were intentional. However, the person in question had problems co-ordinating his avatar's movements. The woman had subsequently made the assumption that standing close to her and in front of her were intentional actions - most people do not usually have a problem controlling their movement in the real world. She had also assumed that the person would recognise that the avatar's actions were making her uncomfortable (as would happen in the real world with cues such as vocal sighs, looks, body language) yet there was no facial or body language feedback for the other person to receive this information. Finally the woman had assumed that the avatar was looking at her - even though there were no faces on the avatars - because this fitted in with her mental model of other anti-social behaviours. The person in question was actually totally unaware of standing in front of her, too close to her or making her feel uncomfortable.

10.4.4 Summary

The research presented in this thesis reveal how the present privacy paradigm is totally inadequate for multimedia communications. Previous research is based upon privacy experts emphasising the importance of *Personal Information*. The majority of multimedia communication is directly personally identifiable (e.g. user's visual image, email address, name etc) yet it would be impractical to treat it all as *Personal Information*. However, some multimedia environments allow for complete anonymity which produces the misguided impression that no *Personal Information* is released and therefore users' privacy is secured. Ultimately the importance of users' misconceptions due to inaccurate social and physical cues relates strongly to users' privacy perceptions.

10.5 SECURITY RESEARCH NEEDS A HUMAN FACTORS APPROACH

This research has identified a lack of social and physical cues (feedback) due to designers' and policy makers' privacy misconceptions. Ultimately, this again highlights the importance of users' perceptions in privacy policy and design procedures. It must *not* be assumed that users will know what is likely to be invasive as they often rely on trust in technology or organisations protecting their privacy. It must not be forgotten that, even though privacy is not an important factor for some, they will react strongly when they see that it has been invaded. This can result in an emotive rejection of the technology and the technology deployers beyond the confines of the present situation. There is a need to counteract these privacy problems before they arise thus solving them before people lose their trust and become emotive about the situation.

Multimedia communication relies on a trusting culture, which allows for the free exchange of information. However, relying on trust to retain privacy within specific media and communities can be dangerous. Privacy invasion may occur unintentionally and be reacted to negatively, not by over-reactionaries but by technology advocates who may just be a little less free with their data next time. This may not mean a solution of restrictive clamping down on multimedia data but conducive codes-of-conduct allowing for users to assess relevant potential *risks*. Communication between the user and the *Information Receiver* with regard to privacy are also required so that a social norm of acceptable behaviour can be constructed. Virtual worlds can be isolating environments requiring new forms of socially communicated norms.

The current discipline of computer security has a technical and military culture which is virtually the antithesis of trust. This security approach has been commented on as a narrow perspective which has produced security mechanisms which are, in practice, less effective than they are generally assumed to be (Davis & Price, 1987; Hitchings, 1995). Study one identified that this authoritarian approach has led to security departments' reluctance to communicate with users with regard to work practices and user requirements. This approach does not fit with modern distributed and networked organisations, which depend on communication and collaboration. However, because of the *enemy within* security culture of many organisations, user feedback is hard to administer (see Chapter 5). The current privacy paradigm, focusing on protecting the individual from malicious attacks, highlights the adversarial nature of the security domain. However, most of my research has highlighted that socially unacceptable behaviours can be stumbled across by a lack of cues to the user and the *Information Receiver* isolating them from the social norms of acceptable behaviour for that specific situation. Often this is caused by poor interface design but also by misconceptions of user perceptions by organisations and system designers. Since privacy perceptions are complex and multimedia communications often defy real world assumptions there is a vital need, now more than ever, to keep in tune with users' perceptions within these environments.

Ultimately, there is a strong need for trust in organisations of the future (Mayer, et al., 1995). This research highlights that if privacy issues are not addressed before they become paramount, this may cause a serious decrease in the trust bond between the organisation and the user. However, those within an organisation most expert in dealing with security rely on a philosophy of non-communication with the user. In order to retain system users' organisational trust levels, they must be informed of potential *privacy risks* (to make accurate *risk assessments*).

10.6 FURTHER RESEARCH

From this research it has been identified that there are three main areas where further research is required. The model factors and concepts demand further, more specific analysis to identify detailed interaction and trade-off scenarios. Further research of these concepts is also necessary within different environments and for different tasks. As shown in the model application (see Section 8.4) further

research can build on and develop the model further. Finally, as noted in Sub-section 10.3.3, the complexity of this phenomenon will result in a reasonably complex model that requires further research in order to identify effective ways of supporting privacy protection and reducing unintentional privacy invasions.

10.6.1 Further research into concepts

The *privacy model* factors outlined within this thesis require further research to detail cut off points with regard to privacy invasion. Future research should identify the predictive elements of these privacy factors. Ethically devised research could identify the sensitivity levels which produce increased invasiveness when viewed by different *Information Receivers* for different usages.

The expert evaluation highlighted that the interaction between information and data requires further research. Specifically, how these two concepts interact to increase or decrease *Information Sensitivity* levels would be useful in the production of effective privacy protection mechanisms. One expert suggested that there was a simple relationship between these two factors. The more data intercepted increased the invasiveness of the information. However, this research suggests that this may be irrelevant, depending on the completeness of the information interpreted. The more data released may increase its contextualisation and actually decrease its invasiveness.

The *privacy invasion cycle* represents an ever-decreasing cycle whereby trust is lowered each time through the cycle until the cycle is broken. Further research is required to identify if this decreasing cycle (spiral) can be broken effectively and how this can be done so that trust can be increased in a contrasting ever-increasing cycle (spiral).

Finally the thesis has identified that current privacy approaches are inadequate for the unique nature of multimedia data. Future research into multimedia communications should identify what they mean by *Personal Information* and identify if this corresponds to users' perceptions of the information's sensitivity levels. Also, further research should not assume that users will know what is likely to be invasive within different contexts but rather detail what will retrospectively increase users' sensitivity levels.

10.6.2 Further research on influencing contextual factors

All of the relevant basic elements of users' privacy perceptions have been mapped by this research so that future research may detail context specific variations. These variations relate, for example, to different domains and tasks (ecommerce, web-site usage). However, further research is required to identify, in more detail, the social norms of acceptable behaviour within different environments and scenarios. How effectively group membership is established and maintained within technology mediated situations is an important factor in perceived privacy perceptions. Further research is also

needed into these issues and to what extent users' perceptions correlate with other group members' perceptions.

Although this research has identified the importance of contextual factors such as organisational culture and national and international norms these issues have not been reviewed in detail. This research has been specifically restricted to UK and US cultural boundaries (see Chapter 1 and Sub-section 8.3.5.8) and further research is therefore required to expand these findings beyond these confines for users from other cultural backgrounds. Indeed the importance of culture within multimedia communications is an important factor that is woefully under-researched and in need of further investigation.

10.6.3 Further research on privacy protection solutions

Finally further research is required to identify effective solutions to the privacy problems and perceptual problems highlighted. Specifically more detailed research is required into pre-emptive solutions to the *privacy invasion cycle*.

The expert walkthrough highlighted that further research is necessary to expand upon the model so that potential solutions are more specific and applicable for designers. Further research is also required to make the model more applicable to generic or shrink-wrapped software as well as situations where development and deployment are separated.