Information and Communication Technologies, Privacy and Policies: An Analysis from the Perspective of the Individual

Thesis submitted for the degree of

Doctor of Philosophy

De Montfort University, Leicester, UK.

by

Sara Helen Wilford

March 2004
Abstract

The Information Society is the result of developments in information and communication technologies (ICTs) and their ability to gather, collate and disseminate vast amounts of personal data. Privacy has therefore become an important social and ethical issue. The threats to privacy include not only the collection of personal details but also the increased use of surveillance technologies, from closed circuit television (CCTV) to email and Internet use monitoring. Individuals have been largely ignored by privacy researchers in the past. This has meant that whilst surveys have revealed some trends in attitude, they did not go far enough to discover how individuals perceive privacy and how far surveillance was seen by individuals as an invasion of their privacy.

This research investigated individuals within a public sector organisation and a private sector organisation. By using a hermeneutic approach combined with the interpretive interactionism tools of Denzin (1989) the research was able to undertake a qualitative investigation of the privacy perceptions of the individual. Furthermore, differences between the approaches to privacy of a public organisation and a private organisation were analysed.

This thesis explores new horizons within the field of computer ethics, and utilises qualitative research techniques not previously applied to this area of enquiry. The research techniques utilised have enabled an exploration of the lived experiences of the individuals within an organisational context. The adaptation of interpretive interactionism within the hermeneutic approach has produced findings that discovered
the importance of privacy and the awareness of the participants to the issues of legislation, protection and future expectations.

The research found that although the individuals studied were happy to allow certain personal information to be available, privacy within the home and within personal relationships was of critical importance. Privacy was seen as a right that all should have, and yet the scope and extent of privacy was subject to individual interpretation. Furthermore, the nature of privacy was seen to have changed with the use of ICTs so that there has been a paradigm shift in the focus of personal information. The perceived loss of community has led to less local knowledge about an individual’s affairs, but the increases in technology have created vast databases containing huge amounts of personal information, which are accessible to many individuals and organisations but to whom the information remains impersonal.
Acknowledgements

I would firstly like to thank De Montfort University for providing the financial support that enabled me to undertake this research and spend time at Harvard University.

It is difficult to know where to begin to thank all the people who have provided me with their wisdom and insight that enabled me to complete this thesis. The journey has been long and on occasion, arduous, and yet without the encouragement and support of so many people, this thesis would never have been completed.

Firstly, I would like to thank Professor Simon Rogerson for giving me the opportunity to start on this journey of personal and intellectual discovery. Without his support this thesis would not have begun. His kindness, sense of fair play and unwavering faith in my abilities made me feel that I really could do this. His leadership has generated a culture within the Centre for Computing and Social Responsibility that provides not only a stimulating intellectual environment, but also a pleasurable working atmosphere.

I wish to thank Dr Lawrence Pratchet, for mentoring me through from undergraduate to completion of this thesis. His friendship and encouragement helped to keep me on track even when things were not going well. Thanks are also due to Dr N.Ben Fairweather whose intellectual challenges were invaluable and who spent so much of his time helping me in the last weeks leading up to submission. In particular his reassurance and assistance during the last few days when things were so hectic was greatly appreciated.
I also owe a huge debt of thanks to Professor Jean Camp of Harvard University, who provided me with the opportunity to spend nearly a year in the exciting and intellectually stimulating environment of Harvard University.

I would also like to thank my children Nuala and Frazer for their patience and encouragement. Thanks to Dave and Deb for their unwavering moral and practical support and willingness to make endless cups of tea. I would also like to thank Heidi and Bernd for reading the drafts, providing comments and typo spotting, and to Mohammed and Xiao Jian for their friendship and encouragement. Thanks also to Lance, Ant, Ian, Wayne, Aimee, Nick, Cath, Ray, Denise and especially my parents Tony and Gill, for never doubting that it would all be OK in the end.

Sara Wilford

March 29th 2004
## Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCSR</td>
<td>Centre for Computing and Social Responsibility</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>CPSR</td>
<td>Computer Professionals for Social Responsibility</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>DSS</td>
<td>Department of Social Security (UK)</td>
</tr>
<tr>
<td>EFF</td>
<td>Electronic Frontier Foundation</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FIA</td>
<td>Freedom of Information Act 2000</td>
</tr>
<tr>
<td>G8</td>
<td>8 Key Democratic Countries</td>
</tr>
<tr>
<td>GEC</td>
<td>General Electrical Company</td>
</tr>
<tr>
<td>HRA</td>
<td>Human Rights Act 1998</td>
</tr>
<tr>
<td>H&amp;BBC</td>
<td>Hinckley and Bosworth Borough Council</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PI</td>
<td>Privacy International</td>
</tr>
<tr>
<td>PLC</td>
<td>Public Limited Company</td>
</tr>
<tr>
<td>Spam</td>
<td>Unsolicited email</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>USA</td>
<td>United States of America</td>
</tr>
<tr>
<td>WWW</td>
<td>World Wide Web</td>
</tr>
</tbody>
</table>
# Table of Contents

Abstract .................................................................................................................................... i
Acknowledgements .................................................................................................................. iii
Glossary ..................................................................................................................................... v

Chapter 1: INTRODUCING THE RESEARCH, AIMS AND EXPECTATIONS ................................ 1
  1.1. Research Questions ........................................................................................................... 2
  1.2. Research Aims .................................................................................................................. 5
  1.3. Structure of the Thesis ...................................................................................................... 8

Chapter 2: PRIVACY, TECHNOLOGY AND THE INDIVIDUAL: AN ANALYSIS FROM HISTORICAL, THEORETICAL AND PHILOSOPHICAL PERSPECTIVES ........................................ 10
  2.1. Historical Overview of Privacy .......................................................................................... 17
      2.1.1. The Individual, from Reformation to Modern Society ........................................... 17
      2.1.2. Privacy as a Right .................................................................................................... 20
      2.1.3. Technology and Society ......................................................................................... 22
      2.1.4. The influence of ICTs ............................................................................................ 23
      2.1.5. Use, Acceptance and Expectations ........................................................................... 29
      2.1.6. How Society legislates technology ......................................................................... 33
      2.1.7. Privacy and Public Policy ....................................................................................... 37
      2.1.8. Commercial Benefits, E-Commerce and the Privacy of the Consumer .................... 42
      2.1.9. Privacy in the Workspace ....................................................................................... 45
      2.1.10. The Trade-Off ....................................................................................................... 49
      2.1.11. Interpretations of Privacy ...................................................................................... 53
      2.1.12. Definitions of Privacy ........................................................................................... 57
      2.1.13. Privacy, Liberty and Freedom ................................................................................. 60
      2.1.15. Privacy and the Freedom to Innovate ..................................................................... 64
      2.1.16. Privacy and Surveillance ....................................................................................... 67
      2.1.17. Privacy and Transparency ...................................................................................... 70
      2.1.18. Privacy: A Social Psychological Perspective .......................................................... 72
      2.1.19. Perception ................................................................................................................ 76
      2.1.20. Organisation ............................................................................................................ 79
      2.1.21. Individual ................................................................................................................. 79
      2.1.22. ICT .......................................................................................................................... 80
      2.1.23. Culture and Ethos ................................................................................................... 81
      2.1.24. Rights ...................................................................................................................... 81
  2.2. Conclusion ......................................................................................................................... 81

Chapter 3: HERMENEUTICS AND INTERPRETIVE INTERACTIONISM: QUALITATIVE APPROACHES TO EMPIRICAL ENQUIRY ................................................... 83
  3.1. Consideration of Research Approaches .............................................................................. 83
  3.2. Hermeneutics: Description and Understanding ................................................................. 88
  3.3. Interpretive Interactionism .................................................................................................. 94
  3.4. Case Study ......................................................................................................................... 102
5.3.6. Access to Personal Information ............................................................ 190
5.3.7. Data Matching ......................................................................................... 192
5.3.8. Closed Circuit Television and Monitoring ............................................... 197
5.3.9. Attitudes toward the Media .................................................................... 200
5.3.10. Age and Position Related Perspectives .................................................. 201
5.4. Concluding Findings ...................................................................................... 203
5.5. Interpretive Interactionism and the Analysis of Selected Individuals .............. 204
5.6. Overview of Individual Perception of Privacy ................................................ 206
5.7. Selection Process of Individuals for an In-Depth Examination of Privacy Perception .......................................................... 208
5.8. Epiphany ........................................................................................................ 210
5.9. Alstec Selected Individuals ............................................................................ 211
5.9.1. Participant A ........................................................................................... 211
5.9.2. Participant D ........................................................................................... 219
5.10. Hinckley and Bosworth Borough Council Selected Individuals .................... 226
5.10.1. Participant M ......................................................................................... 226
5.10.2. Participant Q ......................................................................................... 231
5.11. Analysis of Selected Individuals from a Social Psychological Perspective .... 239
5.11.1. The Presentation of the Self.................................................................... 239
5.11.2. Organisational and Individual Beliefs .................................................... 242
5.11.3. Good or Good Enough? ........................................................................ 242
5.11.4. Articulation of Perception: Interview technique or internal evaluation? ...... 244
5.12. Summary Evaluation of Individuals ............................................................. 245

Chapter 6: FINDINGS AND CONCLUSIONS: A DESCRIPTION OF THE CONTRIBUTIONS AND FUTURE RESEARCH DISCOVERED DURING THIS RESEARCH ............................................................................................................ 247
5.11. Answering the Research Questions .............................................................. 249
5.12. Considerations for the Organisations Studied ............................................... 256
5.13. Considerations for Policy Makers ................................................................. 257
5.14. Overview of the Research: Critique and Analysis ......................................... 257
5.15. Recommendations for Future Research ........................................................ 260
5.16. Conclusion ................................................................................................... 262

Appendix 1 .............................................................................................................. 264
Key Legislation .................................................................................................... 264
Data Protection Act 1998 .................................................................................. 264
Freedom of Information Act 2000 ...................................................................... 265

References ............................................................................................................ 270

Bibliography ........................................................................................................... 289
Chapter 1: INTRODUCING THE RESEARCH, AIMS AND EXPECTATIONS

The information age is sending its tentacles into all aspects of modern society. This research was designed to discover how the individuals in the study perceive this and its impact on privacy of personal information in the information age, individually and within an organisational context both in the public and the private sector. By concentrating on individual perceptions of privacy this research was able to provide valuable insight into the impact of Information and Communications Technologies (ICTs) on privacy perceptions and to consider these discoveries in light of the internal policies and culture of the organisations studied.

Whilst there is a substantial body of work surrounding the subject of privacy there has been little research into individual perceptions of privacy. Yet the way that individuals perceive privacy profoundly affects many fundamental issues in society, from search and seizure laws, to the dissemination of personal marketing data. The importance of privacy therefore needs consideration at all levels. This may be from the individual to government to private business and the judiciary. In this way it is possible to ensure that policies are formulated that accurately reflect expectations and need. Privacy is one of several ‘rights’ that should be taken into consideration and not overlooked en route to achieving policy success.
The effects of privacy loss are being studied in some depth by both academic and non-academic writers. Centres and organisations such as ‘Centre for Computing and Social Responsibility’ at De Montfort University, United Kingdom, ‘The National Center for Digital Government’ at Harvard University, USA and the ‘Electronic Frontier Foundation’ an activist group from the USA are contributing to research and questioning policy decisions. The issue of privacy as a fundamental human right has been analysed and discussed in academic literature. However, individual perceptions have been largely neglected whilst considering privacy from a philosophical, political or organisational perspective.

Individuals are subjected to influences all around them, from television and the media to organisational culture, and from a multitude of other directions. These influences will all have an impact on how individuals feel about privacy. Concern of the impact of ICTs has led to interest in the privacy implications of ICTs and public policy. This research sets out to discover individual perceptions of privacy and the impact of ICTs on those perceptions and to further analyse this in each organisational context.

It became apparent that several questions were central to the research. Answers were sought to these questions during the analysis. These have enabled the research to produce findings that define the initial enquiry and have focused the research in directions that can be clearly stated and yet insightful.

**1.1. Research Questions**

The main focus of the research was to discover individuals’ perceptions of privacy within organisations, with a specific focus on two organisations in the UK which were
the subject of the case studies. These comprised one public sector organisation and one
private sector organisation, in order to provide a contrasting view of each perspective
and to provide insight into the differences of attitude towards privacy depending on the
internal ethos of the organisation involved.

The questions listed below were formulated so that the overall findings were based on
the search for answers to clearly defined areas of enquiry. By drawing together the
findings from each research question and considering these results as a whole it was
possible to discover meaning to the original conceptual questions of individual
perceptions of privacy.

- How do individuals within the organisations studied, perceive the issues
  of privacy and privacy protection?

- What is the relationship between the organisation and the individuals in
  the study with regard to organisational privacy and policies?

- Is privacy considered to be a ‘right’ by the participants in the study?

- Is privacy perceived to be under threat with the use of Information and
  Communication Technologies?

These questions reflect the growth in the ability of new technology to collect, collate
and disseminate personal information and how this has led to a need to consider the
protection of that information for individuals as well as organisations. The UK Data
Protection Act 1998 and subsequent legislation serve to protect individuals from some
of the worst abuses of data collection. Moreover the introduction of European Union
Directive (95/46/EC) 1995, regarding the transfer of data (resulting in the setting up of the ‘Safe Harbour’ principles in the USA and arguably encouraging the growth of privacy protection legislation in countries whose economy is heavily reliant on trade with the EU) has increased the levels of privacy protection for European citizens worldwide.

This research also considers policies within the two organisations studied. The strengths and weaknesses of these organisational policies are identified. Consideration of the policies not only regarding the protection of employees information but also on the protection of information relevant to the continuation of its business, enables this study to treat the organisation as a coherent institution with its own established norms, conventions and culture.

The discovery of organisational privacy culture helps reveal differences or similarities between the public and private sector both in some aspects of compliance with the legal obligations of the Data Protection Act 1998 and the scope and extent of trust the organisation has in its employees. An understanding of the level of awareness and degrees of concern individuals have regarding privacy and its protection, will enable greater care and precision to be brought to bear in future policy making from both an organisational and public policy perspective.

The study indicates some aspects of how well current policies are seen to ensure the protection of personal information of individuals (Bennett, 2000, 2001). The study provides evidence of how individuals perceive privacy, whether it is seen as a right; under what circumstances should the right to privacy be waived and whether there has
been a historical loss of privacy. This work, which analyses the effectiveness of the organisational guidelines for computer, email and Internet use, can be considered to have become more important as access and awareness has increased and the ability to discover information about almost any subject has become more widely available.

1.2. Research Aims

Previous work on privacy has largely concentrated on the ‘right to privacy’ from legal perspectives (Warren and Brandies 1890) and defining privacy from philosophical perspectives. This research concerns itself more with a practical approach whereby individuals have the opportunity to give their opinion on how their privacy is protected, and the importance of privacy to them both as individuals and from within the organisations studied.

In this research two perspectives were taken. Firstly, perception was analysed from an organisational perspective to discern the culture of the organisations studied and the impact of usage policies on the individuals. This enabled the discovery of how important privacy and privacy protection was considered to be within the organisation, not only with respect to employee information, but also sensitive information held within the organisation. Secondly, perception was analysed from an individual perspective whereby views and opinions were considered in the light of how computers had affected personal perception of privacy. Here, the research was able to discover the importance and awareness of privacy at an individual level whilst also considering the concept of privacy as a fundamental right, again from the perspective of the individual participants.
The fieldwork was conducted within two case study organisations where individuals were drawn from across each organisation. An interest in the public policy implications of privacy research meant that the case study involved subjects drawn from both a public organisation and a private organisation in order to provide an enhanced contrast of organisational culture. This enabled considerable comparative analysis to be undertaken and further provided contextual information to indicate the organisational/individual influences on perceptions of privacy. This research presents an analysis of the privacy perspectives of individuals by identifying factors and influences on those perspectives.

By considering perceptions in context, those areas of greater and lesser importance to the participants were revealed. In this way the importance of some issues over others was revealed. The context in which this work was undertaken also enabled the research to discover changes in perception that ICTs had influenced. Further, significant differences between how people implement policies, and how they see the policies in principle was considered to uncover the extent that people’s actions towards others differ from their expectations.

The aims of this research detailed below enabled greater focus on achieving answers to the questions above by reinforcing the areas of enquiry under investigation.

The aims were:

- To analyse the perspectives of the individuals studied in the context of their lived experiences using the techniques of interpretive interactionism.
• To discover the importance and awareness of privacy to the individuals studied.

• To discover the impact of ICTs on privacy perceptions

• To analyse current policies within the organisations studied.

• To analyse the matches and mismatches between policies at an organisational level and expectations at a personal level.

Having set out the aims of the research above, it was important to ensure that the approach and preconceptions were grounded in a solid understanding of the current and established work in the area. In order to place the research into context therefore, a thorough and on-going review of literature related to this area of enquiry was undertaken and is presented in Chapter 2.

The research was approached from a hermeneutic/intuitive perspective which allowed for interpretation and discovery of meaning. This work has combined this approach, and adapted the analytical tools of *Interpretive Interactionism* (Denzin 1989). By adopting an intuitive and interpretive approach to the work, valuable insight has been obtained about individuals and how their perceptions of privacy have been shaped by technological advances. Therefore, the complimentary approaches of Denzin (1989) and hermeneutic enquiry (Gadamer, 1989; Butler, 1998) in interpretation of interview data has enabled a truly intuitive and therefore qualitatively perceptive discovery of individuals’ feelings and personal reactions to privacy and ICTs.
1.3. Structure of the Thesis

This chapter has outlined the questions investigated within this study. It has set out the areas lacking in prior examination by researchers in the field and identifies the aims of this work. Chapter 2 provides a background to the key issue of privacy and considers historical, sociological, theoretical and public policy principles. It examines the effects of implementation, adoption and growth of ICTs and offers definitions to enable clarification of the concept of privacy.

Chapter 3 explains how the approach used for the research was decided and examines the principles in detail. The study sought to move beyond a reliance on theories of knowledge formulated by positivistic processes and into the realm of interpretivism and constructivism. This is utilised by a hermeneutic approach using the tools of interpretive interactionism. The chapter then provides a detailed research model which sets out the steps of the research process and how this would enable the collection and analysis of the rich data needed to provide answers to the research questions.

In Chapter 4 the case study organisations are introduced in detail, setting the organisational scene and placing the research into context. The individual participants are identified and the organisational use policies analysed to further ground the context of the research.

Chapter 5 provides a detailed description and analysis of the study firstly within an organisational context and then from individual perspectives. This chapter comparatively considers the public/private organisations in their own context. By using
the words of the participants this allowed perspectives to be drawn from the individuals within each organisation.

The final chapter presents the results of the analysis and highlights the key findings of this research. In this way, the contribution of this research, its importance and further scope is clearly established. In addition, Chapter 6 contains a critique and evaluation of the research, its limitations and constraints, and offers considerations for decision makers, and future research.
Chapter 2: PRIVACY, TECHNOLOGY AND THE INDIVIDUAL: AN ANALYSIS FROM HISTORICAL, THEORETICAL AND PHILOSOPHICAL PERSPECTIVES.

Recent strides in the development of ICTs have had a considerable impact on society. The information age has seen great advances, in the technologies available to both businesses and individuals. The Internet is one of the greatest innovations. It has made vast amounts of information available to anyone with access to a computer, a modem and a telephone, indeed that Internet access is no longer dependent on the availability of a computer. WAP technology allows the Internet to be accessed through a mobile phone, and interactive television has brought email and web access into homes without a computer.

Huge databases containing extensive personal information are located within both public and private organisations Camp (2000). The growth of information access increases privacy concerns for individuals and organisations, so that ‘concerns about privacy are increasingly about the improper access, use, and manipulation of personal information’ (Moor, 1998 p.16). Identification and authentication abilities combined with facial recognition and other surveillance technologies such as biometrics are continuing to advance so that privacy may be threatened in new and often covert ways.

Transparency and accountability of holders of personal information is becoming more and more expected. The recent introduction and continued implementation of the Freedom of Information Act 2000, gives individuals the ability to demand that their
personal information be made available to them from some public bodies. This also allows access to, for example, financial statements from local authorities.

The growth of information access increases privacy concerns for both individuals and organisations, particularly where that information is of a sensitive or personal nature. The increase in the ability to gather the information and to analyse it, has grown with the ICT revolution where 'the capacity to process privacy-relevant data is much increased' (Fairweather, 2001 p.314). Future privacy protection for individuals may therefore become more difficult to maintain. Calls for access and openness increase with every terrorist act and accounting scandal.

Access to information may have helped in retrospect, to prevent a serious crime. In such cases, it may appear obvious that had the relevant information been made available, tragedies could have been prevented. However, the use of such information and its relevance before an event is no guarantee of success in its prevention. What may eventually appear significant may have seemed unimportant at the time the information was gathered. Calls for such access and openness, often requiring privacy invasive legislation should be considered not merely in light of the media searching for a good story, but as an effective way of ensuring accountability on the one hand, and to aid in law enforcement on the other. However, free access to information may actually increase the incidence of crime where for example, abusive ex-partners succeed in tracking down former partners in order to harass them. There is clearly a need for balance when considering free access to information.
However, there will be some information that may never be exposed to scrutiny. With national security issues, it has been suggested that ‘if we accept society’s opacity we can learn at least to navigate its contours more effectively’ (Turkle, 1995 p.44). This has increased relevance since the events of September 11th 2001. Turkle implies that acceptance of a certain lack of transparency rather than seeking ever more access to information may enable society to find ways of negotiating around problems of too much or not enough information. Therefore, by using our ingenuity and resources in using the information we are able to retrieve more effectively. This approach however may enable public and private organisations to abuse the information, with little challenge or accountability. Further, it suggests a level of deviousness that does not bode well within an open or democratic society.

It is accepted that some transparency and therefore accountability is important and needs to be legislated, even allowing for some restrictions on access as indicated above. Present UK legislation has created a climate whereby there are tensions between the attitudes underlying the Data Protection Act 1998 the Freedom of Information Act 2000 and demands by the media for information. When combined with legislation that clearly restricts privacy such as the Regulation of Investigatory Powers Act 2000 the future of privacy protection for individuals is uncertain.

The individuals studied in the field research and their organisational surroundings are subject to the laws mentioned above. To enable readers to familiarise themselves with the relevant legislation a summary of the three acts appears in appendix I at the end of this thesis.
There is some need for openness and transparency of information whilst maintaining the privacy of innocent individuals. However, privacy may be threatened in many ways. For example, the misuse of information, inaccuracies or over-zealous marketing practices may all be privacy invasive. Privacy is not merely threatened by the amount of information gathered and the use made of it, but the problems of inaccurate, or false information (Camp and Osorio, 2003) which may significantly affect the individual and may impact on their lives. Further, false information given by individuals may increase their privacy but enable crime to be committed anonymously. The use of stolen or fraudulent information may protect criminals through the use of false identities.

There are many threats to privacy as abuses lead to greater steps to identify and control the flow of information. Clarke identifies that the growing threat from identity theft may create further tensions for privacy advocates where the solution to this leads to 'the possibility of routinised self-identification' (Clarke, 1997b p.2). This in turn may lead to the adoption of universal identity cards, thereby losing all anonymity and privacy when undertaking transactions or purchases. Further, there have been recent proposals by G8 nations to develop biometric passports, which would include barcodes, eye scans and fingerprints. This would ultimately be considered for use as a universal identifier. An announcement on July 18th 2003 by the UK government stating that identity cards are to be introduced, means that such a scenario may not be far away.

The use of universal identity cards, particularly smart cards containing large amounts of personal information means that individuals or information about them may become even more easily accessible. This may be to employers, and commercial organisations as well as the police and other public bodies. Being aware of the possibilities is perhaps
one step towards effective policies for the protection of personal information. Access to
sensitive or personal information, and the extent that sensitive information is made
available, will impact on the levels of privacy that individuals can expect and the
strength of privacy protection offered (Data Protection Act, 1998; Fairweather, 2001).

Another kind of privacy that may be threatened is that of ‘associative privacy’ (DeCew,
1997). This is distinct from information privacy as it involves interpersonal
relationships and the ability to be intimate. This form of privacy may be threatened by
surveillance such as the use of CCTV and where ‘the right to establish and develop
relationships with others (Neimietz v Germany, 1992, 16 EHRR 97) reinforces the idea
that privacy vests in people not places’ (Taylor, 2002 p.76). As will be discussed later,
during the field research, this kind of privacy was considered in most contexts to be
more important than informational privacy by the interview subjects.

The potential for the chilling of relationships and intimacy that surveillance presents in
all its forms means that a ‘lack of privacy and confidentiality has a chilling effect on
user’s choices’ (Gardener, 2002 p.3) and can therefore be considered more potentially
damaging to individuals than informational privacy. The need to develop friendships
and intimate relationships with family members, the ability to argue or to engage in
sexual activity in private is considered critical to well being, dignity and to maintain and
develop familiarity with other individuals.

Protecting the privacy of individuals and organisations requires continuous re-
evaluation. This rapidly changing world where ICTs play such a huge role, and where
this is expected to increase, requires a vigilant approach to privacy. As technology
develops and the ability to obtain personal information gets easier, it is perhaps inevitable that some individuals will abuse these abilities. The academic focus on Computer Ethics led by respected researchers such as James Moor, Deborah Johnson and Simon Rogerson is important in raising awareness of the many different aspects of computing that permeate our lives. In ensuring this, ‘applications of information ethics must be broader, more profound and above all effective in helping to realise a democratic and empowering technology rather than an enslaving or debilitating one’ (Bynum and Rogerson, 1996 p.135).

Whilst a relatively small number of people around the world can be considered information rich, the information poor number many billions. The quantity and quality of the information available to those with access is immense and ‘information empowers those who have it but it also disenfranchises those who do not ‘(Rogerson, 1999 p.3). The Internet produces an overwhelming amount of information, much of which may be trivial and inaccurate with little way to ascertain its truthfulness or validity (Collste, 2000). Almost anyone who has ever searched the web cannot fail to notice the huge amount of seemingly irrelevant web sites that are found during searches.

Privacy issues arising from such huge amounts of information and its largely unrestricted access means that some information that was previously only available in the public domain in paper format could be no longer appropriate when disseminated electronically. Information such as phone numbers and personal details, previously requiring long hours of research in public libraries, now only take minutes online to discover. This makes it much easier for the idly curious to discover personal
information as 'if it just takes 15 minutes on the Internet, the temptation to snoop is greater' (Spinello, 2000 p.105).

There are therefore many different issues concerning the use, implementation and development of technology and the potential for privacy invasion and protection. An awareness of the positive as well as the negative aspects of new technology use is necessary in that privacy invasive technologies may provide more efficient information or enable a safer environment to be maintained (Thomson, 1975; Etzioni, 1999a,b, 1997; Spinello and Tavani, 2001; Sirianni and Friedland, 2001). Striking a balance is a key element in this and the chapter will reflect and evaluate different views on these issues.

This chapter identifies the historical and philosophical roots of privacy and the individual, and discusses the importance of privacy, socio-political and cultural development in Western industrialised society (Fromm, 1942; Prosser, 1960; Fried, 1968; Winner, 1977, 1992; Elias, 1997). It further discusses and identifies the implications of increases in technology, which have the ability to directly impact on the privacy, liberty and well being of individuals (Orwell, 1948; Fried, 1968; Miller, 1971; Lyon, 1994; Edgar, 1997).

In summary, this chapter identifies and discusses those key concepts of computer ethics that effect an individual’s perception of privacy and technology. It summarises the historical roots of privacy, and debates the theories of technological determinism. This chapter introduces the key elements of the legislative framework, which aims to protect but may not ultimately succeed in that protection (Fairweather, 1998). Finally, there is
an analysis of the ‘right’ to privacy, and a clarification of the meaning of the key terms ‘individual’, ‘perception’, ‘privacy’, ‘organisation’ and ‘ICT’ that are used during this research.

2.1. Historical Overview of Privacy

2.1.1. The Individual, from Reformation to Modern Society

It has been suggested by some, that privacy may not always have been important within Western European society (Fromm, 1942; Etzioni, 1999). In the past, people lived, worked and worshipped in close proximity to each other. The nature of privacy was not really explored until the concept of ‘individuality’ arose during the Reformation. This period around the 15th century saw many changes in the way people perceived themselves and how they behaved. Prior to this, Fromm (1942) indicates that there was no privacy or freedom for any individual. There were restrictions, decided at birth, indicating the manner of dress, food eaten, guild, and many other areas of life. ‘In cities, sumptuary legislation designated what dress different urban groups should wear so as to keep them separate’ (Spielvogel, 2002 p.1).

Prior to the Reformation in medieval Europe there was no room for individuality. Everyone knew their place in society and was not allowed to deviate from their predetermined path. During the reformation, the initial ‘primary ties’ (Fromm, 1942 p.20) which connected individuals to society and family began to become less permanent and more fragmented. The concept of individual privacy may have only arisen due to individuals being isolated from their previously close-knit communities.
whilst at the same time being physically surrounded by large numbers of individuals
with whom they had little or no connection or interaction.

If one has always been used to living in small open communities then the
transformation to largely autonomous family units, living in an urban environment
could appear disturbing (Maffesoli, 1996). This would serve to create a focus on the
individual or small semi-autonomous family units rather than the community as a
whole. Fromm (1942) also indicates that the new found freedoms of this time created
fear in the general population and solutions to this ‘excess of liberty’ were sought in the
Calvinist and Lutheran religious doctrines (Calvin, 1979) which arose during this period
in response to uncertainty (Spielvogel, 2002 p.1). Although often restrictive in nature,
these religious communities provided a sense of belonging, which may have been seen
as more important than any subsequent loss of freedom. Other responses to the changes
at that time reveal that activity was often ‘channeled into finance, industry, and the
rationalization of a broad range of productive activities’ (Winner, 1977 p.112). The
increase in economic activity allowed individuals to use this newly discovered freedom
to increase personal wealth and security.

The movement away from the medieval tenets of original sin, and therefore a lack of
free will, to the growth of humanism developed by scholars such as Erasmus and
Thomas Moore, (Hart, 1991 p.1) was perhaps critical in the development of the concept
of the individual. It is particularly important since for many, freedom was not
something they were accustomed to, and so probably did not perceive its lack, but rather
feared its appearance. For those embracing freedom, opportunities were suddenly
greater. Individuality and the ability to think and behave in those terms was an
important advantage during this period of change.

Historical overviews provide a background but what is also important in this thesis is to
relate the importance of privacy to the more recent developments of the use and
implementation of Information and Communication Technologies.

In today’s society, people lead contradictory lives. There is a perception of need for
privacy and autonomy (Cooke, 1999) whilst maintaining a desire to participate and
belong in society. This may be due to two elements. Firstly, the cramped and busy
lives we lead create a desire to escape from the hustle and bustle into somewhere safe,
tranquil and private (Miller, 1971). Secondly there is a need to belong and to participate
or to receive social welfare benefits. People willingly comply with requests for
information within the surveillance society (Lyon, 1988, 1994, 2001), and as members
of society are aware that participation ‘require the information to be given and that the
ends to be achieved are worth the price of diminished privacy’ (Bloustein, 1964 p.185).

Another possible reason for participation may be the desire for material gain such as
money off coupons and bonuses through store loyalty cards, which may become
available to those willing to give up some portion of their privacy as ‘users are promised
certain goods in exchange for personal background information’ (Spinello, 2000 p.108).
During this research it became clear that consumers do not always associate their
participation in surveys to receive money off coupons, with the increase in junk mail
arriving on their doormat. On the other hand, it also became clear that counter to this
desire for participation and material gain is a desire for protection of personal
information, or those elements of privacy that each individual consider vital to retain some degree of personal autonomy. It is this dichotomy that makes the formulation of privacy legislation and decisions on levels of protection so difficult.

It is not possible for us to turn the clock back to some pastoral ideal (which probably never actually existed in the way we imagine it). Privacy within modern western society is now so important to the individual that in many cases, ‘loss of privacy is loss of dignity’ (Miller, 1971 p.49). A lack of privacy can result in problems such as diminished personal relationships, a lack of motivation, secrecy and a chilling of innovation. In light of such potential problems privacy should be considered critical to the survival and development of society and the maintenance of personal autonomy.

2.1.2. Privacy as a Right

The right to privacy, its scope, need and nature has been debated long and hard. Ethical questions are often examined independently and yet privacy and the right to privacy are frequently included within discussions of liberty (Mill, 1992) or natural rights (Forester and Morrison, 1995), without being considered separately. Locke, (1968 p.43) suggests that there are three fundamental rights, life, liberty and property. Hart (1955) when considering natural rights saw liberty or freedom as a fundamental human right but did not explicitly refer to privacy.

Thomson (1975) considers that privacy is nothing more than a property right, which one can retain or dispose of in much the same way as any other possession. However, Fairweather (2001) considers this ideal view position to be flawed and that ‘children should be entitled to sexual privacy of a sort that it would not be acceptable to buy or
sell’ (Fairweather, 2001 p.310). Fairweather’s concerns clearly indicate the problems of Thomson’s theory where it is not considered within a broader context. Privacy therefore cannot be interpreted as the same for everyone as different perspectives offer different evaluations.

Even if privacy is considered a right, there are differing opinions on the extent and scope of its interpretation. Etzioni (1999) for example, indicates that privacy is not as important as the values and priorities of society as a whole and that ‘giving up some measure of privacy serves the common good’ (Etzioni, 1997 p.1). The Communitarian perspective indicated here therefore considers that ‘individual rights need to be balanced with social responsibilities, and that autonomous selves do not exist in isolation, but are shaped by the values and culture of communities.’ (Sirianni and Friedland, 2001 n.p).

However, as mentioned earlier, the field research revealed a remarkable consensus that privacy is a right, with all respondents considering this to be important.1 Writers such as Miller (1971), Edgar (1997), Gandy (1993) and Oz (1994) consider privacy to be more important from an individual perspective, whilst considering that societal considerations should be taken into account. In this view it is the effect on society of a

---

1 The nature of privacy as a ‘right’ was not explored in detail during the interviews. This was because the focus of this research was to discover perceptions of privacy and the impact new technologies have had on those perceptions, and not to discover the depth of philosophical understanding of the participants, which would have gone beyond the scope of this research. However, the interviewees did indicate some caveats as to the extent that privacy is a right, and this will be discussed later during the analysis in chapter four.
lack of privacy for individuals that may create problems. A lack of some level of privacy, as mentioned previously may be problematic for an individual’s sense of autonomy (Miller, 1971) and well-being (Edgar, 1997). The very act of reducing individual privacy could well cause a more secretive society, which may create a breeding ground for dissent, disruption and terrorism (Fromm, 1942 p.221). Thus, without some areas of confirmed rights to privacy, society may find that some individuals come to behave in more secretive and covert ways to counter the lack of privacy.

The diversity of opinion on privacy and privacy rights suggested a need to debate issues of privacy from differing theoretical perspectives. The aim of this section has been to present current thinking on privacy issues and the historical influence on those perspectives. The conclusion drawn suggests that rights and privacy are socially constructed ideas, which are open to interpretation dependent on cultural, social, philosophical and historical influences. Privacy is not merely a property right or tort as seen by writers such as Thomson, (1975) and Prosser (1960) but a more fundamental need for individuals in that ‘a presumption must be given to privacy rights instead of property rights because human dignity is at stake’ (Spinello, 2000 p.124).

2.1.3. Technology and Society

The discussion above reveals the need for privacy particularly within modern western society. Interpretations and definitions of privacy that highlight the stance taken in this research are offered below (p.55-59). For this thesis however, it is equally important to discover the effect ICTs have had on privacy and how the individuals within society
view privacy. ICTs may either enhance or diminish privacy according to how it is used and developed. What is important is how society may control the development and implementation of new technologies (Winner, 1977, 1992; Heilbroner, 1994) in order to protect privacy. Whilst there are considerable concerns as to the nature and need for privacy as mentioned by Etzioni, and others, it is necessary to discuss and to explain the increase in the implementation and development of ICTs and how its development may have impacted on perceptions of privacy

2.1.4. The influence of ICTs

The manipulation of flint and stone and the development of crop and animal husbandry as technologies for increased food production may have created the idea that individuals are beings with specific skills beyond those of pure survival such as hunting and gathering techniques (IHP 1, 2002). Over the generations these skills, or at least the inquisitiveness to acquire them by repetition, trial and error and so on, would make some members of a group stand out as individuals with specific skills. These people would become known as the local blacksmith or potter. Individuality is not particularly relevant at this time. This, as explained earlier would come at a later point in history.

In ancient civilizations such as Greece, there was a high degree of organisation and society. This has come to be seen as a direct precursor to modern western democratic civilizations (Barrow, 1999). In nature ants form complex societies with a hierarchy and monarchy. Ant society at such a primitive level is in no way interested in the individual. The queen and her individuality, is only as important as the office she bears, and has no ‘personal individuality’ of importance within the hive.
The very nature of our ability to express our individuality by using tools, which enabled a permanent record to be maintained, ‘with the invention of writing in about 3100 BC’ (IHP 2, 2002 p.1), has further allowed a greater consistency and continuity of knowledge. This has spurred generations to look further and further for greater knowledge.

Technology is not limited to recent innovations in computers or the hard sciences. Technology can be anything that is used or derived to make something simpler, more accessible or to increase production. This can be something relatively simple such as an axe or a complex tool like the printing press. Technology therefore may be merely a tool to facilitate change. The use of tools as a way of achieving a greater level of production and/or efficiency means that there may be a degree of inevitability about technology and its advancement. This is further tied in with the curiosity, ideas and nature of a society in which goods become essential through familiarity with that technology. A good example, given by Winner (1977 p.84) is the car, which has become almost a necessity within Western society, and yet is a mere technological invention of a previous age.

Heilbroner (1994) believes that the tying up of technology with production means that technological determinism i.e. where technology drives forward and determines its own path, can be directly related to economic determinism. What economic determinism says is that within capitalist societies, the need for production, and the value placed on increases in production will drive technology forward. Moreover as information becomes a commodity to be bought and sold as a product, and as the availability of
information increases through the use of ICTs the impact on the ability to protect the privacy of sensitive information is highlighted.

The history of civilization and its development can be traced to a long time before the industrial revolution. Certainly, ancient civilizations used technologies, which were subsequently able to benefit and drive forward the development of society. It can be suggested however, that there is a predictable force of development and progress. The rate and nature of any change in society, whether brought about by changes and developments in technology or other factors such as climate, war, or political upheaval, is however unpredictable. Winner (1977) would refute Heilbroner’s economic determinism approach, by indicating that he is forgetting the fundamental desire of individuals for freedom of choice. By contrast according to Winner (1977), Ellul (1964) considers the economy to be powerless in its influence on the growth and development of technology.

Winner argues that Heilbroner’s focus on economics and production does not consider the values and beliefs of a society and its culture and this will have a bearing on the outcomes of any technological advance. Heilbroner (1994) however suggests that if the belief systems and attitudes within the elites of society harmonize with those of the technologists, then society will drive technology forward. This indicates a perspective that goes beyond his originally stated economic determinism theory.

Technology can be described as having three key perspectives that can explain its continual change, development and implementation:
1. **Nonnative accounts** - Here technology is an influence only if society, its culture and politics encourage and add meaning to that technology. In this way, technology is driven forward by the technicians and will continue apace if society evolves the same ideas and standards of judgement.

2. **Nomological accounts** - in which technology itself drives itself forward ‘In nomological accounts, the technology-driven society emerges regardless of human desires and values’ (Heilbroner, 1994 p.84)

3. **Unexpected accounts** – or the unpredictable nature of change

(Adapted from Heilbroner, 1994 p.84)

Ellul (1964) argues that there is little society, or individuals wishing to participate, can do to slow or prevent its proliferation. Technology in his view is seen as a roller coaster, which once begun is almost impossible to stop and has ‘fashioned an omnivorous world which obeys its own laws and which has removed all tradition’ (Ellul, 1964 p.14). Some concession can be made to Ellul’s concerns, which were articulated prior to the computing revolution and can now be seen as insightful particularly if a technological deterministic approach is seen as valid. In some ways, Ellul can be seen as predictive when we consider technological advances since the 1960’s and the proliferation of computing technologies since the invention of the silicon chip. His implication that we are incapable of determining our path and must merely adapt however does not allow for individual autonomy and innovation. Moreover it does not consider that technology is developed by people and not imposed by some outside influence. However, what is certainly true is that as each advance is developed it is easier and more likely that further developments will be born out of the previous ones.
A different and perhaps more palatable view of the continuing drive forward of technology is that held by Castells who states that ‘Technology does not determine society: it embodies it. But neither does society determine technological innovation: it uses it’ (Castells, 1996 p.5). This approach indicates a more rounded and sympathetic view of technological advancement. It also gives some hope to society that it may be able to control technological change or at least the direction of that change so that technology may benefit society rather than being defined by it.

We can consider that society and technology are a mutual driving force, one driving and being driven by the other. On further examination it becomes clear that society has developed a tendency to facilitate these advances further with the development of an infrastructure. The infrastructure enables technology to advance in areas such as banking, insurance and the labour market. This can be considered in the light of Heilbroner’s economic determinism, although it does not imply that economy determines technological change rather that technology, society and economy are mutually driven. As Winner states, ‘In modern society men and institutions readily embrace inventions and discoveries and take steps to see that they quickly become innovations in the broader sphere of practical activity’ (Winner, 1992 p.74). Winner’s view differs considerably to that of Ellul (1964), who considers that the individual may see technology as the driving force, seemingly without conscious control. Winner (1992), Castells (1998, 1996) and others therefore consider that society and individuals may ultimately control innovation and thus the ability to decide what is developed and that is the view maintained during this work.
In this view we adapt and change each innovation as it is developed, with economic and social forces influencing and being influenced at the same time. It can be surmised therefore, that technology, or at least change, may be cyclic in nature whereby society, change and production perpetuate each other. The term ‘Technological drift’ (Winner, 1977 p.88) suggests that technology does not drive itself forward. Technology develops without anyone really noticing until it is already embedded within society and each generation inherits the previous generations’ technology and advances it.

This however could be considered a worrying trend, where there is some loss of autonomy and choice over technology. Once again this indicates that some form of technological determinism may be at work. However, it should be remembered that the choice of technology is not the same as the advancement of technology, and whilst the majority of individuals may have little choice, the elites in society make choices on their behalf. In this way some individuals, by their inclusion in that society ultimately will have some influence. Technological advance however, is usually brought about by the innovation of individuals or small groups who then provide society with the products of their invention (Popper, 1959; Winner, 1977; Williams, 1995). The decision makers within that society, the economy and other factors such as the environment, influence the choices made thus completing the cycle of influence.

This analysis of technological adoption however further serves to accentuate the need for control of personal information and the maintenance of some private realm and autonomy. As members of society, individuals accept this lack of control as being the price for participation within an established community. From a technological
perspective, 'few citizens or consumers wish to be excluded from the network of information flows' (Lyon, 2001 p.108).

Winner, Ellul and other scholars in the field (Mac Murray, 1968; Gandy, 1993; Lyon, 1988, 1994, 2001; Oz, 1994; Edgar, 1997; Heilbroner, 1993; Castells, 1996, 1998) may have subtly differing views on the reasons for technological change, advancement and the effect this will have had on privacy and society. To ascertain a correct one is difficult. On consideration, the stance taken in this thesis is that 'although technology has a force of its own, it is not independent of political and social forces' (Regan, 1995 p.12). In this way society drives and is driven by technological change in a cycle of influence. Therefore, there is a certain inevitability of continued innovation, which is also influenced by social and economic demands combined with the availability of resources both intellectual and material.

2.1.5. Use, Acceptance and Expectations

ICTs, from the development of the telephone to more recently the Internet and the World Wide Web, have made society more global. Individuals, who are widely dispersed globally, can interact with each other and research practically any topic quickly and in some depth. The use of the Internet enables individuals to 'greatly expand the opportunities for research and investigation' (Spinello, 2000 p.28). An example is the creation of high speed global networks, such as those offering real time, low cost support and information to families and individuals suffering from rare diseases. This was impossible until the advent of ICTs. In this way, global tribes may be isolated individually, but by participating in the use of ICTs they are able to become
members of geographically distant and diverse but cohesive groups. The Internet therefore is ‘helping create a new social and economic order that is characterized by global connectivity and the decentralization of authority’ (Spinello, 2000 p.ix).

The use of computing technology greatly increases the scope of each individual participant. This can be through the use of the Internet to gain knowledge and information, the use of a personal home computer to keep a track of the household budget, or merely as an outlet for recreation and game play. It cannot be denied that the increasing power of computers is changing and challenging us in more ways than we would have ever thought possible. We need therefore to be concerned that society must seek to control as well as use these emerging technologies as ‘we are not, indeed, locked in. But there is a slope, an incline in things that is all too easy to slide down’ (Taylor, 1991 p.101). As Taylor indicates here, the benefits of new technologies are immense, and yet so are the possible dangers that are represented by the technological revolution.

Possibly one of the greatest problems within modern western society and its use of new technologies is a lack of general awareness of the potential threats to privacy and security that such access may bring. ‘The Internet provides a whole new set of specific ways in which people's privacy may be intruded upon, and adds new dimensions to existing problems’ (Clarke, 1997 p.7). An example is where an individual may be vulnerable to incorrect data files on them particularly where there are inadequate levels of protection, recourse and accountability. This vulnerability may only become evident years after the incorrect or intrusive data has been obtained. Incorrect data may only be revealed if credit is refused or a job application rejected. However, the information may only come to light if the individual concerned carries out an investigation. It is
important to consider therefore that ‘A general principle that characterises fair
information practices is that data subjects should be able to access their personal
information with an ability to amend if necessary’ (Bennett, 1992, p.101).

In some cases however, this incorrect information may never come to light but may still
affect the course of someone’s’ life. The requirement that individuals must actively
seek out the information being held on individual databases means that people may find
it extremely difficult to correct or remove information on them. This is because such
data may exist simultaneously in numerous places. Where this occurs it may
‘compromise the individual’s capacity to defend him or herself or to prosecute his or her
innocence’ (Clarke, 1997 p.13). The problems of incorrect information may also create
problems much later in life. An example is where an individual has paid into their
government retirement scheme where e-government is in operation. If the information
is held on a computer, and the data input clerk put in the wrong information, it may be
that none of their contributions have been placed into their account. In such a situation,
someone reaching retirement may find that their pension is not what they were
expecting. Without sufficient correction facilities embedded in the long term plans of e-
government systems, it could prove time consuming, expensive and distressing to
uncover and correct.

The networking of databases may also create further problems where incorrect or
misleading information is held or where the creation of databases means that threats to
privacy arise from the ‘recombination of disparate and hitherto unconnected data
elements’ (Spinello, 2000 p.105). Each database may contain only a sub-set of the
information, or may match such information in order to create an individual profile,
which could lead to false positives, where innocent people are singled out for increased scrutiny by security agencies. There are many permutations and conclusions that may be derived from just one set of data. Although it may be possible to correct information, it is not so easy to alter profiles and matched data, which may not contain references directly to the incorrect data, but contains inferences and presumptions based on that data. Therefore protection of information privacy, particularly where data is matched to create a profile requires ‘acknowledging our systematic inability to identify the data subject as being the same as the moral self with which the data subject identifies itself’ (Van den Hoven, 1997 p.430). This highlights the difficulty of data matching that considers an individual as a ‘profile’ which may not reflect how the ‘real’ person sees themselves.

An area of growing concern, particularly in the USA is that of identity theft (Garfinkle, 2001; Camp and Tygar, 1999). This involves the discovery of some personal information such as an individual’s social security number, name and address. Much of this personal information is relatively easy to obtain through the Internet. In cases of identity theft, individuals may lose money, reputation, or credit rating. In some serious circumstances their liberty may be lost, as the criminal may commit other more serious crimes in their name. The reclamation of one’s personal identity after such an attack can be very difficult, and may require the changing of one’s name and personal details if the attack has been particularly severe. An awareness of the potential for abuse of personal information, and the measures that can be taken to minimise the risks are therefore essential in order to participate safely. Most of us are unlikely to ever experience such an attack, but safeguards are necessary none-the-less, to ensure that we are protected.
2.1.6. How Society legislates technology

Technology and society can be said to drive each other in a cycle of influences, from innovation and implementation, to adaptation and legislation. Problems arise however as inevitably the speed of technological innovation exceeds the ability of society and the legislature. The legislature within western society has often behaved reactively to each new technological advance and ‘the legal system...has lagged behind the steady erosion of privacy’ (Spinello, 2000 p.109). Attempts to introduce regulations and guidelines of behaviour hopes to discourage the abuse of those new technologies. David Lyon observes that, ‘the need for constant vigilance is met by various movements that attempt to challenge each new development whose negative aspects are recognised’ (Lyon, 2001 p.131). The awareness and activities of those generally seen as opposing change is important to balance the proliferation of technologies whose uses may be detrimental to society. What are also needed however, are counter balances that see the benefits that the same technologies may bring, and an awareness of how over-zealous legislation may affect the civil liberties of society. In this way a rounded and well-informed approach to legislation can be achieved.

There are however problems in that technological change often moves ahead of the ability for society and its various groups, to adapt or properly grasp future implications of the technologies. This can create ‘policy vacuums’ and ‘conceptual vacuums’ (Moor, 1979 p.266). It can also cause problems for society, which may create reactive legislation that is ill-conceived, inadequate or privacy invasive. This may be due to the lack of sufficient frameworks in place to enable decision makers to understand ethical
problems that may arise from computing and ICT technologies, or a lack of knowledge about the technology and its potential.

A technologically deterministic view may be taken by decision-makers who fear a lack of control, since superficially; the driving force may appear to be the rapid take-up and proliferation of technology. Elias (1997) made an interesting related observation when he stated that ‘Mankind’s process of learning about the unplanned things happening to it is a slow process which trails considerably behind the social process in which it is engaged at any time’ (Elias, 1997 p.165). What is of concern here, is not that technological determinism may be correct as a hypothesis, but that its implications may be re-interpreted by ill informed decision makers to justify the suppression and/or rejection of technology, science and inquiry.

The rate of technological change however cannot be accurately predicted, and any attempt to restrict technological progress is generally resisted. This resistance, particularly by those at the cutting edge of innovation is necessary as ‘technology is most productive when its ultimate range of results is neither foreseen nor controlled’ (Winner, 1977 p.98). As previously argued, both society and technology can be seen to drive advancement, and this may be regardless of its positive or negative long-term effects. Unexpected consequences, both good and bad, might arise from any technological change.

To reiterate, it is not therefore technology per se which drives itself forward, but a huge array of factors in the cycle of influence. These include the history of the society in which it is developed, the perceived needs of society at the time, the socio-political
environment, and the past technological developments, which enable further innovation. Any legislation resulting in the chilling of invention, discovery or development within society may serve to undermine the progress of future generations. An interviewee from one of the case studies highlighted perhaps the key principle behind the continuation of technological advance when he stated that ‘you can’t un-discover or un-develop something that has been discovered or developed’ (Interview 2, subject Q 2001).

The legislation of technology is however necessary particularly when it has been implemented into society where opportunists will abuse systems, and where the full implications of a technological advance are not realized until after its implementation and immersion. Legislation may occur after there has been some form of abuse, or concerns have been raised. A good example would be Patriot Act 2001 in the USA, which was passed due to the attack of September 11th 2001 and which served to push the legislative wheels forward.

Legislation may also be necessary where commercial or consumer interests may need protection as with the UK Data Protection Act 1998. Other forms of legislation may be deemed necessary that enable individuals to gain access to files kept on them by governments’ and other public agencies such as through the Freedom of Information Act 2000. This, combined with privacy protection, in the guise of data protection laws may create a minefield of apparently contradictory legislation.

Cosmetic policy making by the state such as that of the UK Data Protection Act 1984 served to obscure privacy problems and violations. As is the nature of cosmetic policy
making, the Act itself was almost entirely without teeth with little in the way of resources available to ensure compliance or punish those who did not comply. The improvements made by the introduction of the Data Protection Act 1998, under considerable pressure from European Union directives may have a more positive effect on privacy protection. However, without sufficient resources, it is unlikely that the Information Commissioner can properly enforce the Act. It should also be noted that infraction of the Act will probably only surface once someone has complained, indicating an on-going problem within an organisation and only represent the tip of the iceberg. It is also likely that many infractions would go unreported.

It should be mentioned at this point that the Regulation of Investigatory Powers (RIP) Act 2000 heralds further privacy erosion within the UK. Although seen as a way to attack crime, particularly through the use of ICTs and the Internet, the threat to civil liberties and the potential loss of privacy may be of concern. The Human Rights Act 2000 however may serve to contradict and therefore alleviate some of the potentially serious implications of the RIP Act. However, as no test cases have come to light to date, time will tell as to the true impact of these two pieces of legislation in combination.

It is important for compliance and to prevent misinterpretation that there is an understanding of the relevant legislation with regard to personal information and privacy. This is particularly important when considering the scope and extent of the Internet and email use policies in the organisations studied. An in-depth analysis of the legislation however goes beyond the scope of this research. It is necessary however to
summarise those Acts that may impact on internal policies and they can be found in appendix I.

2.1.7. Privacy and Public Policy

Colin Bennett (1995) indicates that decision-makers often underplay the public policy implications of privacy. Public policy issues should not ignore privacy concerns, particularly where information technology and information systems are considered. Bennett indicates a need for a blending of theories and research to enable good legal protection of privacy including social awareness as indicated by Rule (1973). This should be combined with a public policy approach (Bennett and Grant, 1996; Bennett, 1995; Pratchett, 1997) whereby ‘moving away from the purely practical, and delving into the theoretical, enables the development and understanding of privacy as a major public policy issue’ (Bennett, 1995 p.32).

Public policy however, is a practical discipline. Those who make policy decisions impact the lives of individuals in many ways, often affecting the quality of life of large groups of people. Awareness and consideration of privacy and the protection of privacy is therefore fundamental when making far-reaching policy decisions.

During the research, it was immediately clear that the Local Council employees were taking privacy legislation very seriously, with training and workshops for all being implemented at the time of the study. What was revealed from the interviews was the reluctance of councillors to attend these training sessions. ‘Councillors were down to go on it as well and we’ve not been overwhelmed by their response to the training so far’ (Interviewee Q, 2001 p.2).
Whilst there is no way to be sure that this is not just isolated to this particular council, it is perhaps indicative of a trend amongst politicians to see privacy as considerably less important than other issues. Whether this is because they do not see this as potentially vote winning and therefore unimportant, or whether it is apathy, or that privacy issues are considered low priority is unclear and was not examined during the study. What was revealed however is the impact that an awareness of privacy issues had on those Councillors that did attend ‘But those that have been, have been quite frightened by it’ (Interviewee Q, 2001 p.2).

What this reveals is that once the issues of privacy and data protection are brought to the forefront, those decision-makers who perhaps previously had not considered the issues in depth; began to consider the wider implications more seriously. There is also an indication therefore, that higher levels of training and education are needed. This would serve to raise general awareness of the implications of not protecting privacy and personal data. Moreover, it would highlight the greater need of political decision makers to address the issues of privacy more seriously.

The works of Pratchett (1997), Webster (1998) and Lyon (1988, 1994, 2001) attempt to identify the issues of the information age at policy level. The scope of such work ranges from the use of surveillance technologies to the identification of pressures on governments to use systems for information gathering.

Their work highlights the critical issues that face governments and decision makers where policy and needs have to be balanced with the rights of the citizens to prevent the loss of rights or freedoms, and to ensure redress when things go wrong. In this way
there is a need for swift intervention at the governmental policy level, rather than leaving it to theorists to argue the toss. As Colin Bennett states, ‘privacy is an important right that the state has some obligation to protect through regulatory policy’ (Bennett, 1995 p.31).

Policy formulation, however, is often a slow process and legal and public policy processes may be seriously lagging behind the rate of technological development. However, policy can occasionally be extremely reactive and be changed without due consideration of the implications of its implementation. The rapid deployment of the Patriot Act 2001 in the USA shortly after the terrorist attacks of September 11th 2001 is a good indication of reactive policy making. In this way, policy can be either lacking in proper consideration of delay on the one hand, or too rapid implementation on the other. Both scenarios can seriously damage the citizen’s right to privacy, and their ability to protect it.

It has not been established that privacy is a fundamental right. Privacy may be considered vital in a society where individuals live in close proximity to each other. The threats to the fabric of society if privacy intrusions are allowed to go unchecked are great, and ‘there should be a reasonable prima facie expectation of privacy’ (Fairweather, 1999 p.42) whether in the workplace as Fairweather indicates here, or in our interactions with government or business.

Other arguments such as those espoused by Communitarians would indicate that public policy and the public or community good is always the most important consideration. From this perspective the implementation of the Patriot Act in the USA and the RIP Act
in the UK are justified regardless of the subsequent losses of privacy, as they will lead to greater levels of community protection. However, civil liberties groups and privacy activists such as Privacy International, and the Electronic Frontier Foundation, would disagree. Therefore the consideration of the privacy needs of individuals will enable the free flow of ideas, lead to innovation, and preserve dignity.

Government has encouraged us to see ourselves as consumers, providing us with large amounts of information through the Internet. The introduction of the Freedom of Information Act 2000 has also provided each citizen with the right to access information held on them in public sector departments such as local councils. This has all been undertaken with the idea that individual ‘consumers’ should take responsibility and demand certain standards in the provision of services.

This combined with the provision of some redress when things go wrong has transformed the provision of public services in the UK. The privatisation process largely instigated during the 1980’s and 1990’s enabled reinforcement of the consumer culture. Privatisation was intended to increase competition and thus value for money. The consumer society however, may have opened the door to control and manipulation by business interests, whilst leaving any form of accountability largely to market economics. This may mean that ‘the processes of democratic government have been subverted by the producer – dominated oligarchies which control the welfare state’ (Bellamy and Taylor, 1998 p.91).

Moreover, citizens as consumers may be manipulated negatively, and the freedom of choice espoused by the government may actually lead to a lack of real choice. This may
be due to the market being seen as more important than the quality of services being offered whereby ‘citizenship in the information age consists of…the registering of consumer preferences’ (Bellamy and Taylor, 1998 p.92). Within the Environmental services department at the local council studied, it was indicated that the constraints of market forces on the provision of services such as refuse collection, had led to a culture which insisted on the lowest possible price for a service. This had led in some cases to the service provision being reduced in quality. The ‘McDonaldisation’ of public services, may have had the opposite effect to what was intended. This may have led to cut corners, poor services and unhappy consumers rather than the empowerment of consumers and the ability of councils to consider bids for the best services at the lowest prices.

The link between commercial enterprise and public service has served to blur the boundaries between them. A major privacy concern here is that if potentially sensitive information is collected on behalf of a public sector body, by a commercial one, there is a potential that the public may not have the same rights to access their information under the Freedom of Information Act 2000 as they would have otherwise. Also, the access to such information by commercial business ‘can serve as the building block for richly detailed customer records’ (Spinello, 2000 p.107) and which may lead to a greater chance of increases in junk mail, Spam, unsolicited phone calls and direct marketing. The sale of names and addresses of potential customers is still a problem, which means that there must be a great deal of caution as to the extent that private business should be involved in the provision of public services.
1.8. Commercial Benefits, E-Commerce and the Privacy of the Consumer.

The commercialisation of goods and services may have served to reinforce the ideology of the individual and the development of a self-serving ‘me’ culture. This means that individuals and organisations have been encouraged to consider only themselves and what they can get out of a system, product or service with little or no thought as to the potential harm this may bring.

The West is largely a consumer society, and the concept of citizenship may be lost to the notion of market forces and consumerism (although there are moves to incorporate citizenship studies within the schools National Curriculum in the UK perhaps in response to concerns for this). The strength of commercialism and consumerism means that there is much scope for manipulation by industry so that consumers are conforming to an increasingly dominant corporate power seeking its own ends’ (Mac Murray, 1968 p.viii).

1.8.1. Data Matching

Businesses use our previous purchases in the retail sector to act as a guide for our references; it follows therefore, that a presumption may be made about what our future choices may be. If we are later offered products that reflect our preferences, there is then a reduction in the scale and extent of choice. It has already been established that there are limits to our choices based on previous innovation and choices made by previous generations (Winner, 1977). However, our choices may be further limited by organisations that use our previous purchases as indicators, match that data with other
ata, and produce a profile. This information is a great tool for business as it allows the
marketing of their products and services to be directly targeted to a specific audience.

However, there are problems here. Computer-based profiles may not necessarily reflect
the real preferences of individuals. A product may be purchased and disliked and never
bought again, the product may be bought for someone else, or individuals may not
actually ‘fit’ the profile. The use of statistics aims to show the mean or average of a set
of data. Often, the mean of a data-set will not actually be able to produce an individual
profile that accurately complies with the mean. In the same way, data matching may
lead to an unclear and inaccurate picture of preferences and purchasing habits that may
indicate averages and likelihood, but do not refer to real individuals or consumers.

Data collected using consumer questionnaires may be useful to industry to ascertain the
preferences of their customers providing ‘a major source of marketing data to reach
selected groups of consumers’ (Spinello, 2000 p.107). However, responses to such
questionnaires may be less than accurate. There may be several reasons for this.
Respondents may give answers, which they feel are expected of them, which may be in
order to obtain some form of payment or concession, which the respondent desires.
Also, such questionnaires may be completed at a stressful time such as when out
topping with children. This could encourage answers to be given without
consideration in order to get it over with as soon as possible. It is therefore possible that
de data collected may be imprecise and unable to truly convey the preferences of the
dividual concerned.
Another area, which may cause concern, is that of television subscription. The idea of each consumer being able to choose what they will watch at any time may appear to increase the ability of the individual to exert control over this aspect of their lives and freedom of choice. However, all may not be, as it seems. The potential for the targeting of particular societal types in the audience grows as the scope and variety of inputs is reduced.

The danger of ‘narrow casting’ in this way may cause sectorisation of society, creating groups of people whose views on a subject may be determined by the type of channels subscribed to creating a ‘complex discrimination technology’ (Gandy, 1993 p.132). If people only watch certain types of channel and do not have any alternative input, the danger may be that society can be more easily coerced into accepted patterns of behaviour whereby the ‘repetition of slogans and emphasis on factors which have nothing to do with the issue at stake numb his critical capacities’ (Fromm, 1942 p.112). However, individuals still have the capacity to turn off the television or not engage in the use of data gathering technology.

In today’s society however, it is difficult to envisage how it may be possible to avoid some form of participation unless one lived in isolation on a desert island. As Brenton suggests, ‘a man’s home may be his castle…but in a credit economy it cannot help but be built along goldfish bowl specifications’ (Brenton in Miller, 1971 p.67). As the desert island is not an option for the majority, it is the responsibility of decision makers to control the extent to which it allows the gathering and use of personal data whilst continuing to enable participation within the information society.
1.9. Privacy in the Workspace

The legally permitted commercial use of computerised records for marketing purposes and the active monitoring in the workplace of employees' telephone, email, and computer may indicate the lack of importance historically given to privacy as an area in need of consideration. Some corporate policies such as intensive workplace monitoring whilst seeming profitable, or efficiency boosting, may directly infringe on the privacy and autonomy of the individual. As Spinello states 'there is a real danger that the workplace is becoming a panopticon where workers activities and interactions are transparent to the corporate hierarchy' (Spinello, 2000 p.121).

The long-term effects on staff may eventually bring about the opposite effect to that envisaged at the beginning. This may involve low morale, lack of trust/feeling trusted, absenteeism, high staff turnover and high stress levels which may result in lower levels of efficiency and profitability. Dejoie, Fowler and Paradice (1991) and Lyon (1994) suggest that the dangers of monitoring of employees may include fear, unrest and high staff turnover. This could eventually undermine an organisation's ability to function or progress effectively, by creating a culture whereby creativity and innovation is oppressed due to an over reliance on rules, procedures and close monitoring. However, on a more positive note, as indicated by Rosenberg (1999) 'it is possible to create environments that value worker's integrity, respect their privacy, moderate their stress level, thereby achieving higher productivity while ensuring that management's interests are protected' (Rosenberg, 1999 p.9).
Research into organisational computer use policies and how they are interpreted and understood by employees will help towards an understanding of the relationships between policies, implementation throughout the organisation, and individual perceptions of privacy and autonomy. This is because 'conflicts exist between the needs and expectations of the individual and the obligations and roles of the organisations and agencies that perform key functions in any complex technological society' (Forester and Forrison, 1995 p.131). An awareness of the disadvantages as well as the advantages of the implementation of new technologies is important for both employers and employees where 'digital networks pose significant threats to worker autonomy as well as opportunities for its enhancement' (Brey, 1999 p.15).

Computing technologies have had considerable influence on business and how employees work within that business. The use of the Internet, mobile phones, laptop computers and the availability of video conferencing have made the possibility of working away from the office a reality for some employees. The flexibility experienced by these workers is at first glance very great, with the ability to work as and when they fit, and providing the opportunity to fit family and work into more convenient slots during the day.

This picture however, may not be as rosy as it is painted. It cannot be denied that some greater degree of freedom for employees and efficiency for employers may be afforded through the use of ICTs. Teleworkers have been shown to save around US$10,000 per year in the provision of office facilities in a central business district (McClelland, 1999). However, it can be argued that one of the most immediate threats the use of ICT for the monitoring of workers presents is the loss of privacy. This loss may be informational,
societal, philosophical or individual. The impact on the individual where the lack of privacy is directly due to employer monitoring in the workplace or the encroachment on social or family time for remote workers is one, which is of concern.

Society has not been technologically capable of serious privacy violations on a large scale for very long. It was this technology gap that defended the privacy of personal information. However ‘we seem to be entering a new era in which there is a diminished respect for these workplace rights such as privacy’ (Spinello, 2000 p.121). The threats to individual privacy therefore are becoming greater with potentially damaging techniques such as data gathering, portfolio building and surveillance. As Marx states, ‘just because privacy expectations are historically determined and relative, it is a fallacy to assume that they have to become weaker as technology becomes more powerful’ (Marx, 1998 p.3).

The relationship between employer and employee is a contractual one. The importance of this must not be understated. The essence of the contractual relationship is of an agreement entered into by two consenting parties. It is considered a basic right of free individuals to decide whether or not they wish to enter into such a contract without the interference of others. Despite this freedom the employer-employee relationship is highly regulated within most legal systems. This regulation is motivated by several aspects, such as the importance of a stable labour market and the need to promote well-being and security among employees.

One of the purposes of regulating the labour relationship is therefore, to ensure that the relationship is mutually beneficial and not preserved by force. Regulation has
gressed and adapted to ensure that the relationship finds its balance in each stage of social and technological development. To ensure balance, governments have regulated items like the minimum wage, working conditions and worker integrity. However, as stated earlier, there is always a considerable lag between the developments of new and potentially privacy invasive technologies and the regulatory system. Workplace monitoring on the scale that is being experienced by some employees, particularly those who use computing technology in the workplace is developing and being implemented at a greater rate than regulation can keep up to protect those employees.

That is unclear at present, despite an awareness of contractual obligation and legal restraint on an employer, is whether the employee will check email or answer the phone beyond working hours due to perceptions of need, or through a feeling of obligation to the employer. It should also be noted that the culture in which the employee works may have a distinct bearing on the level of obligation felt by the employee to the employer. This may be over and above any contractual obligation on the part of the worker and legal restraint of the employer.

There is a need to re-evaluate the rules because the social and technological norms in a society are in a constant state of change. Technological developments may move society along and leave law and ethics struggling to catch up. Or as Justice Holmes wrote ‘it cannot be helped, it is as it should be that the law is behind the times’ (Holmes, 19034 n.p).

This phenomenon has been called ‘cultural lag’ (Ogburn, 1964). Ogburn observed that material culture advances more rapidly than non-material culture. Examples of the
tter are religion, ethics, philosophy, law and values. The former, material culture
connotes physical equipment and the procedures for using and producing the
equipment. According to Ogburn there were four major driving forces of social change:
Invention, accumulation, diffusion and adjustment (Marshall, 1999). The advances in
material culture force society to eventually re-evaluate non-material culture. But before
this re-evaluation takes place there is a gap within which outdated non-material culture
rattles to fulfill its purpose.

The law provides an excellent example of the importance of cultural adaptation since
the rules, once established, represent an ethical norm of a fixed time. The law is
therefore outdated as soon as it is created. To overcome this serious obstacle, legal
scholars have created a solution explained by Justice Brandeis in that, ‘in most matters
is more important that the applicable rule of law be settled than that it be settled right’
burnet v. Coronado Oil). In saying this he meant that the old non-material rules must
ot act in such a way as to be counterproductive once the material culture has evolved.

1.10. The Trade-Off

The ability of corporations to monitor employees even across great distances has now
come a reality. The main goal of the corporation is profitability particularly whereby
employees have very few rights with respect to workplace privacy’ (Rosenberg, 1999
6). The need for employers to consider the welfare of employees has, despite much
proved employment law within the western world, often become secondary to the
creased output potential. Remote workers and those employed within the confines of
computer monitored realm, may reap huge benefits for the company. It has been
estimated that teleworkers are ‘20% - 45% more productive, and the direct costs of employment are $5000 - $8000 less per annum’ (Hodson, 1995 p.1). The computer monitoring of remote workers is further reducing supervisory costs to the employer and enhances profitability.

With the advance of monitoring comes the decrease of trust. Trust is a reciprocal relationship (Luhmann, 1979) and has even been referred to as the lubricant of society (Arrow, 1974). The employer who is too mistrustful of his employees will only breed a feeling of mistrust and disloyalty among his employees. This in turn does not allow for the optimum work result from the employees. To remedy low performance many companies attempt to use surveillance technology, which again decreases the level of trust in the relationship.

Within the privacy debate employee monitoring has been discussed from a technical, ethical and legal point of view. Despite the lack of clear figures it has been estimated that between 15-30% of American companies monitor their employees (Hodson, Englander and Englander, 1999). For the most part, the debate on employee monitoring as concerned the ethical and legal rights of employers to monitor employees.

The monitoring has involved, among other things, reading of email, scanning computer files, measuring keystrokes and closed circuit television (Lyon, 1994). The employers usually claim that they have the right to monitor their employees. This right is based upon the traditional hierarchical view of organisation where the concept was that people did not want to work and needed to be rigorously supervised (Ciborra, 1993).
his attitude led to the building of hierarchical organisations where the supervisor’s
main role was to ensure that the employees actually carried out the work that they were
aid for. The employer’s right to monitor is an historical claim based upon the
organisational forms from the early industrial society. This right has been upheld in
many laws and courts in varying legal systems. The question is not whether they have
his right but rather how far they can go while exercising the right. Workplace
monitoring which can severely limit the privacy of an employee can also have serious
fects on well being and motivation. Research has shown that ‘monitoring worsened
employee morale and thereby negatively affected performance’ (Hartman, 1998 p.6).
his clearly indicates that the scope and extent of employee monitoring should be
onsidered, not so much in the light of what can be done, but more by considering the
ential for detrimental effects on the monitored.

he right to monitor employees is based upon a traditional view of labour organisation.
However, the technology which is in use has become much more sophisticated and
ere has been a shift in the manner and subject of what is monitored. As employers
egin to take a greater interest in not only the work time of employees but also their
free time’ it is perhaps of concern that ‘we see a pattern developing which really
comes an issue of technological control which can take on Orwellian proportions’
Brown, 2000 p.62). In the traditional hierarchy the supervision concerned itself with
fact that employees were actually present, performing adequately and that no thefts
urred. With the advances in ICT, employee monitoring has become an efficient
oductivity-measuring tool, which can be used to measure both work output and
ality. This right to monitor employees has not been unquestioned (see for example
odson et al, 1999).
Such employment law is years behind the technological capabilities for monitoring and remote working. It is therefore the responsibility of employers to ensure that their employment practices are ethical and ultimately most likely to get the greatest long-term return on investment. If this is disregarded in the search for the ‘fast buck’, businesses may find that the price may be high staff turnover and recruitment problems, stress-related illness and low morale. This may then lead to a less efficient and thus less profitable organisation.

The effects of having and using workplace technology in the home is to undermine the division between home and workplace and therefore works against the separation of work and free time. The need for privacy and free time is important for the worker's ability to focus efficiently on his work and therefore produce more value for the company in which he is employed.

While there is little or no legal support as yet for the overuse of workplace technology in the home this should not deter us from the argument. One reason is that there can be no legal development unless there is a debate on the issues first. It should be considered that ‘conflicts exist between the needs and expectations of the individual and the obligations and roles of the organisations and agencies that perform key functions in any complex technological society’ (Forester and Morrison, 1995 p.131). The law is in itself a codification of what society (or a segment of society) feels is just at a given moment. This means that the law is a record and reflection of what society believed to be true at that time. The debate therefore is whether previous legislation and opinions would be used to impede future social and legal development.
In summary, there is a real need for employers and employees to be aware of the possible dangers of overwork that may arise through the ability to work 24 hours a day. The concept of ‘all work and no play’ which if taken literally means that Jack really is in danger of becoming a ‘dull boy’ without some relaxation time. Further, ‘without privacy, autonomy will be consistently threatened and enervated’ (Spinello, 2000 p.122) and ‘respect for the autonomy of others is a moral imperative that cannot be arbitrarily relaxed or overridden for the sake of economic expediency’ (Spinello, 2000 p.122). The future with regard to innovation and inspiration is potentially in jeopardy with the losses of privacy that accompanies some new working practices. The damage to the individual, family, and society may also be far greater than previously envisaged in a world where to be successful in a career may involve some radical choices, between becoming a work automaton and having a life beyond work.

1.11. Interpretations of Privacy

The countless attempts to define privacy suggest that privacy is one of the more objective issues for analysis in this age. It is difficult to define for several reasons. Privacy means very different things to different people depending on their perceptions, state of mind and circumstances. There is no agreement on a universal standard even in legal terms. ‘The right to be let alone’ (Warren and Brandies, 1890 p.205) has often been cited as the first real attempt to identify privacy and its need for protection. When seen in its historical context however, it is discovered that its main focus was with regard to media intrusion into the personal lives of public figures and not a generic term to cover all aspects of privacy. Privacy covers a much wider area than that of the purely public sphere.
Rosser (1960) considered privacy law to be more concerned with tort, such as defamation, intrusion, false publicity and the use of a name or image rather than an area of legal protection in itself. This contrasts with Thomson's view (1975) that privacy is nothing more than an aspect of property rights. Bloustein (1964) however argues that privacy may be of a more ethereal nature and that it is the actual invasion of privacy that is of concern and not the effect of that invasion. 'The gist of the wrong in the intrusion is not the intentional infliction of mental distress but rather a blow to human dignity, an assault on human personality' (Bloustein, 1964 p.165). Further, the invasion of privacy may increase the risk of mental distress. Fried indicates that intimacy and trust are impossible without privacy and that 'depriving one of privacy destroys the possibility of bestowing the gift of intimacy' (Fried, 1968 p.216).

An individual may be left alone (as in the Warren and Brandeis definition) in some sense and still have their privacy infringed by the collection, matching and subsequent use of personal data for marketing or investigation purposes. Also, data, which may have been freely given, may be used in privacy invasive ways if it is then re-processed and used for a different purpose from that initially intended. Although the Data Protection Act 1998 prohibits this alternative use, it is not clear whether investigation or prosecution is undertaken without complaints first being made. Where individuals are aware of the infringement of the Act it is difficult to enforce. Therefore, that someone may be left alone in a physical sense is not sufficient privacy protection in today's surveillance society whereby privacy invasion can be undertaken remotely and without the individual's knowledge or consent.
privacy violations may also occur without the individual’s knowledge as in the case of peeping toms. In this instance, not being aware of being watched does not mean that the victim’s privacy is not being invaded. From one perspective, there is a possibility of image to the individual in the way they are perceived by the watcher. This may be as a sex object or a figure of amusement, or may impact on other aspects of the victim’s life if the watcher is in a position to influence future events such as access to services where ‘sensitive information collected without one’s permission and knowledge can be a potent weapon in the hands of those in positions of authority’ (Spinello, 2000 p.103).

An example of this is if a security officer for an apartment block could secretly watch a tenant going about their daily business. The observations and perceptions of that person may result in the watcher behaving differently towards them than he would otherwise.

Another perspective as indicated by Fried (1968) is that an individual may be damaged in an ethical or ‘spiritual’ sense, whereby the harm is done by the very act of privacy violation regardless of any awareness or disadvantage to the victim.

His analysis however only serves to clarify that privacy may be violated whether or not the victim is aware of it. The definition of privacy itself however, is not so clear cut. There are so many different opinions on what actually constitutes privacy, as will be observed below, that defining privacy is notoriously difficult. What is helpful for this search however is the ability to discover some of the key indicators, which will help to develop a working definition of privacy for this thesis. The interview analysis yielded many insights to be discovered about individual perceptions of privacy, what is considered fundamental and what is not important or less important. The research results mean that the following discussion of privacy definitions is considered not
urely from a theoretical perspective but grounded in empirical evidence of general agreement in the research results.

It is relatively easy to state the benefits of privacy for the individual. Rossiter (1958) considers that privacy provides the individual with 'independence, free will, secure autonomy, dignity and resolve against the whole world' (Rossiter, 1958 p.24). This statement suggests the need for privacy but does not actually define privacy. Rossiter seems to be suggesting that privacy is a right and need of an individual, but his statement may also be seen as confrontational, insular and unrealistic given the round nature of society. The concept of independence and resolve against the world does not allow for balance and co-operation, nor does it allow that individuals within society need to participate and so must perhaps give up some of their privacy (Lyon, 1994; Campbell and Connor, 1986).

Philosophy has attempted to make sense of the needs of society for some level of privacy. However, technological breakthroughs in information and communication technologies (ICTs) mean that philosophical theory may have been unable to adapt quickly enough. The winds of change within philosophical theory may have a tendency to blow very gently and slowly, with philosophical opinions often based in theories, which are thousands of years old. This tends to guard against short-termism, yet the speed at which society changes particularly within the realm of new technology is rapid. His is not to say that Socratic and Platonic precepts are not helpful. Such theories may be useful for their basic interpretations of morality and ethics, but they may be unable to deal with the complex changes in society within the last few decades. Therefore,
Philosophy may only be useful as a preliminary tool for the development of computer science and privacy theory.

While definitions of privacy may abound, they are perhaps not as important as a practical awareness of what is important and why. The discovery of what is actually expected to maintain a sense of well being is likely to indicate the effect the implementation of protection policies, legislation, the media that new technologies may have. In this way, privacy concerns should always be considered during the earliest development stages of a potentially sensitive project to ensure that controls are built in rather than bolt on.

1.12. Definitions of Privacy

This selection of definitions below is just a small representation of the multitude of different opinions and perspectives that privacy takes. This is the main problem of course, when trying to define and eventually legislate something as subjective as privacy. Each one of these definitions, and the multitude of others all have a slightly different view on what privacy is, how far it should be protected and where the boundaries are between privacy and isolation, or privacy and secrecy.

The right to be let alone’ (Warren and Brandeis, 1890 p.205).

The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’ (Westin, 1967 p.7).
The limitation of others' access to an individual with three key elements: secrecy, anonymity and solitude" (Gavison, 1984 p.421)

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

'Freedom from intrusion or public attention' (Concise Oxford English Dictionary, 1990)

There is considerable confusion and disagreement surrounding the theoretical and ethical debate on privacy. This identifies a need for discussion of the issues within the study of privacy to identify present trends and allow for the future development of privacy theories. How individuals see the world they live in has an effect on what is perceived as being a valid theory. However, philosophical discussion can be concerned with the discovery of the right theory regardless of public perceptions. As those who formulate theories are also a part of and influenced by the society they study, perceptions of issues will have an effect on the development of theories. The clearer the evidence becomes, through research and analysis as to individual perceptions, so theories can be developed which reflect rather than proscribe. Society consists of individuals and therefore individual perceptions allow for a greater degree of understanding of society. The work undertaken here to discover individual perceptions of privacy therefore provides insight that serves to further enhance the study of privacy theory and the development of definitions.

Since there are no universal agreements concerning privacy at this time, the problem is to find a starting point at which all would accept privacy as important, necessary and in need of special consideration to prevent its erosion. It appears that despite attempts to
ise awareness of ethical and privacy issues by organisations such as Privacy
International, and writers such as Lauden (1995), Spinello (2001, 1997, 1995), Raab and
88), privacy issues are still sidelined by policy-makers and largely ignored by the
edia.

hile such as Almond (1995) and Glover (1977) have analysed ethics from the
osition of contemporary philosophy, largely drawing on the foundations laid by Locke,
t and others in allowing that there may be some rights, which could be considered
iversal. In trying to define privacy and to discover its importance and nature, a
arting point in this research then was to consider that privacy is not necessarily a
ight', but something we have come to expect, or an ‘emotional state’ (Miller, 1971).
the United States of America constitution there is no explicit reference to the right to
ivity of the individual. Subsequent judicial precedent and legal rulings are the only
anisms by which the US constitution protects privacy. However, the analysis of
se research revealed that whilst philosophical theorists may not consider privacy a
ight, there was a full agreement of all participants that privacy is a right. The problem
defining privacy as a fundamental belief in consistent terms, and with clear
arameters, was however in no way so clear.

he issue of privacy, which may not have been considered important historically
romm, 1942) may, in modern society be critical to the well-being and autonomy of
ividual (Oz, 1994; Gandy, 1993). One may consider what a person sees as
ivy, as loneliness and exclusion, or as a way of hiding wrongdoing. This again
uld suggest that privacy is subject to an individual’s perception, as is any definition.
That can be considered is that privacy itself may have become a right as the need for it is grown, but the degree of privacy that should be protected is dependent on individual perceptions, culture, and religion. This means that it is difficult to protect or define privacy to a universal standard.

Trona (1996) notes that it is often presumed that privacy is important but not why. Traditions may play a major role in deciding how rights are perceived and to whom they apply. There are questions to be answered surrounding the issue of privacy and how far current ethical theories have developed to accommodate the computer age.

So we really need or desire privacy in a modern transparent society? As previously stated, privacy is a relatively modern concept, which can be said to have developed due to a desire or need to escape from the strictures and tenets of modern society. The idea that one may wish to 'escape' may be unacceptable in the usual sense, in that it conjures up an image of instability and an inability to cope. However, it can be suggested that this need to escape is a way for an individual to come to terms with what may be seen as an unnatural existence.

1.13. Privacy, Liberty and Freedom

Privacy and liberty/freedom are not synonymous. Privacy is concerned with the ability to withhold information about oneself. Liberty and freedom however, are concerned with the ability to do what one wishes; perhaps under certain constraints such as those proposed by J.S. Mill (1992) in that no 'harm' shall be done to others. Liberty, like privacy is a subjective issue. According to Berlin (1969) in his seminal work 'two concepts of Liberty', there are two main concepts of liberty, 'positive' and 'negative'.

60
some respects 'negative liberty' has become enhanced by ICTs. This may be particularly evident with the use of Closed Circuit Television (CCTV) cameras and the advances in facial recognition software.

Negative liberty is described as the ability to go about one's business unconstrained by others. In this way, only those wishing to perpetrate 'harm', operating outside the accepted terms of liberty, should suffer any loss of freedom. Since we do not live in a state of societal chaos in the west, the criminals’ loss of freedom to do as they wish is seen as legitimate. Therefore ‘It cannot, of course be asserted that the preservation of freedom at the expense of some addition to our present material comfort will be thus awarded in all instances (Hayek, 1944 p.38).

As society continues to grow and develop privacy to some extent must be relinquished to facilitate the efficient use of technology. Lyon suggests that ‘to participate in modern society, is to be under electronic surveillance’ (Lyon, 1994 p.4). However, as we further become embedded in the ways of modern society, there may be a related loss of liberty, autonomy and freedom whereby ‘the price he pays, however is high, it is the loss of his self’ (Fromm, 1942 p.160).


The research conducted during this study indicates that individuals do not consider formation privacy an important issue; although it is considered a 'right' (A detailed analysis of this can be seen in Chapter 5). What should be considered however is the effect that the media, education and other factors may have on perceptions. Individuals are bombarded with positive images of information transparency, which can also be
translated into personal security (as in the use of closed circuit television, or more
personalised services in the case of marketing and preference surveys, and internet
cookies'). In such circumstances individuals may be less worried about privacy than
they would be if they were given a more balanced view, which included the negative
aspects of these technologies in the same measure. The concern here is that such
positive images may not indicate other possibilities with regard to the use of these
technologies. This may involve potentials for the tracking of individuals who may not
have committed a crime but who may be seen as undesirable due to their political views
or if an error in the input or processing of information leads to credit refusals or
inappropriate medical care.

It is important therefore to understand the distinction between what individuals think
and how they are perceived to react by media and information suppliers. These groups
have an interest in ensuring that the information they produce is believed and possibly
accepted upon. Therefore, they may wish to direct the tone and scope of information
depending on the target audience. The use of the media may mean that individual
perceptions of what does and does not constitute an invasion of privacy may be based
on populist impressions or commercial marketing bias. However, consumers would be
better informed by clearly reasoned ideas based on the pros and cons of an issue
received from an impartial perspective. The relative lack of debate however, has
assured that the issue of privacy is largely ignored.

The Orwellian dystopia of the book 1984 (Orwell 1948) warns of a society so
constrained by the fear of someone knowing everything about them that it forces
individuals to behave in an expected and proscribed manner. Another dystopic
Possibility is that society could become so dependent on the use of ICTs that individuals may become unable to function autonomously, relying on external forces to make our voices for us, as in Aldous Huxley's *Brave New World* (1950).

The concept of automatic and accepting citizens could also become a potential breeding ground for extremist politics. As elements of society try to break away from one form of totalitarianism and stumble into another 'the despair of the human automaton is fertile soil for the political purposes of Fascism' (Fromm, 1942 p.221).

The previous discussion suggests that society has reached a stage in its development whereby issues of privacy and freedom must be accepted as a right. The problem arises, however, when the scope and extent of the protection is considered. How far privacy should be protected however may depend largely on the perceptions of privacy and liberty as a whole within society.

Some degree of privacy is an ideal, allowing for the development of individuality and innovation through the ability to retreat from observation and scrutiny. This private calm enables the individual to return to view, once they feel that it is appropriate rather than being obliged to operate in a purely transparent and therefore to some extent, restricted way. Mill as an example indicates 'in each person's own concerns, his individual spontaneity is entitled to free exercise' (Mill, 1992 p.85).

There is disagreement as to the validity of privacy at all, let alone an agreement as to a universal definition. Introna offers an explanation of privacy as 'the idea of some personal space, some area, within which one is free from the gaze and judgement of
...hers' (Introna, 1996 p.204). This definition, drawing on J.S Mill’s work on the nature of liberty, has been expanded for this study. It includes the ability to withdraw oneself from external influences and to independently consider oneself as an individual free from the constraint of societal expectations. This withdrawal by the individual into an internal realm of the self is where the perceptions of each individual may be discovered, and may be the only truly private realm available to individuals. Thus, privacy may be seen as an internalisation and protection of the self, formed and influenced by the boundaries of our experiences. For the purpose of this research, it is helpful in the identification of external influences on the individual’s perceptions of privacy.

1.15. Privacy and the Freedom to Innovate

In a modern day surveillance society, there are some basic tenets of privacy, which may be challenged. Etzioni (1999) for example sees privacy to be a problem for society, and that one should only consider personal privacy in the light of the common good, or the community. On a psychological level, a challenge to privacy may be the privacy of individual thought. This may initially appear to be the last bastion of complete privacy and autonomy. Individuals are constantly influenced by input of information, from before we are born and throughout our lives, from external stimuli such as T.V, reading material, personal relationships and economic circumstances.

‘There is no real freedom of thought in our society, so it is said, because the opinions and tastes of the masses are shaped by propaganda, by advertising… and by other environmental factors, which inevitably force the thinking of the people into well worn grooves.’

(Hayek, 1944 p.122)
his view, proposed by Hayek in the mid 20th century was based on society at that time, and although it was written during wartime, it can be seen as a prescient comment on the future of society in a commercialised world. What Hayek could not have foreseen however, was that computing technology would further embed commercialisation and mass consumption within society. Inclusivity has been encouraged by governments and corporate interests so that the goal of western society has become the desire for all to be ‘connected’ which makes mass manipulation easier to achieve.

There may be less obvious influences on our thoughts than computerisation, such as inputs from the environment and food. Alternatively, our own perceptions of ideas and ideals may originate in our unique chemical make-up as well as through our life experiences and choices. Many factors will undoubtedly have an effect upon our thoughts and actions. It has recently been suggested that even propensity to criminal or anti-social behaviour may originate in our genetic codes. This may mean that our responses and even our deepest ‘private’ thoughts may not be truly private.

Some of these influences may come from sources with a vested interest in making us think’ in a certain way. If this is so, maybe it is already too late to perceive privacy as anything more than an internal sense of ‘self’. Concrete thoughts may be no more than conditioned reflex, along the lines of Pavlov’s dog, whereby we react to stimulus in a reconditioned manner. Fortunately, human beings have some ability to behave autonomously, even when influenced by corporate or governmental manipulation or media propaganda.
ome form of privacy is necessary for society and the individual. A totally transparent society whereby individuals are merely parts of a system and where independent thought is discouraged, may threaten historical gains in individuality and autonomy. In his way individuality and autonomy are severely threatened. Fromm identified the problems for the individual in a society without privacy and, therefore, freedom, when he stated that ‘the right to express our thoughts, however, means something only if we are able to have thoughts of our own’ (Fromm, 1942 p.207).

he potential for manipulation and conditioning identified above indicates that even our thoughts may be predictable in a society where much personal information is known about us. Stereotyped reactions and preferences may indicate a loss of free will and therefore a lack of privacy in many of our thoughts. In such a society ‘the sense of childhood is diminished and freedom is constrained’ (Lyon, 1994 p.194). Such is the anger of a society without privacy.

In a personal level, privacy may be required to ensure the sanity of the individual. Sanity in this sense is the ability to maintain a balanced perspective on life. As Edgar states, ‘Privacy may simply be necessary to mental survival, just as the body needs sleep’ (Edgar, 1997 p.225).

he previous discussion demonstrates the need for control and balance to ensure a functioning society (Agre, 1994) where the individual is not isolated through too much privacy thus divorcing them from society and disabling the ability to interact and participate. Further individual autonomy should not be undermined by mass participation to the exclusion of individuality and innovation. It is accepted that there is
often a need for team-work and collaboration for many of the innovations within many aspects of society. However, the need of the individual to be able to spend time alone and in contemplation, not merely for spiritual growth but also for intellectual growth is clear (Frankena, 1973; Feinberg, 1969). It is not possible for an individual to share all aspects of themselves and not to lose something unique. This uniqueness gives us the ability to innovate, speculate and formulate ideas. This would not be possible if individuals were always expected to work as a group thereby diluting ideas into those acceptable to the majority.

1.16. Privacy and Surveillance

The issues of privacy and ethical computer use are becoming more important in society. Often only small pockets of academia and activists are aware of the threats to privacy. An example is the lack of resistance to Closed Circuit Television (CCTV) in the UK. CCTV is 'the use of video surveillance cameras and systems in public places where camera technology is linked in ‘real-time’ to a control room containing monitoring and storage equipment' (Webster, 1999 p.3). The use of such technologies may directly infringe on the privacy of the individual and could result in ‘the societal panopticon of the all-seeing state’ (Bellamy and Taylor, 1998 p.18). Lyon further enunciates this view when he states that ‘surveillance progressively replaces physical coercion as a means of maintaining order and co-ordinating the activities of large populations’ (Lyon, 1994 p.3).

A balance between loss of privacy and freedom, and participation in a supposedly safer environment is therefore required. This double-edged sword of issues is sharply felt
nder surveillance and is of particular relevance to the development of Closed Circuit Television (CCTV). Berlin indicated an awareness of this kind of conundrum when he stated that ‘the freedom of some must at times be curtailed to secure the freedom of others’ (Berlin, 1969 p.126).

‘CCTV, however, is not alone in enabling surveillance of the population. Lyon (2001. 994, 1988), Marx (1998) and Spinello (1998) indicate that any form of data gathering and information retrieval may directly infringe on the privacy of an individual and constitutes surveillance. If that information is abused then any act of surveillance may be considered an invasion of privacy. This may be due to the altered actions and actions which may occur when someone knows that they are surveyed. An example here is of Jeremy Bentham’s Panopticon. This was a design for a prison involving a central hub for surveillance with cells placed rather like the spokes on a wheel. The guards could see the inmates, but the inmates could not see the guards. The principle being that if the inmates think they may be under surveillance, they will behave accordingly.

Another point, which is particularly relevant to the use of CCTV and other forms of surveillance, is that the individual, who is under pressure from the impermanence and wide range of opportunities of the modern age, may feel a high degree of fear, insecurity and helplessness (Fromm, 1942). This then means that ‘the striving for security tends to become stronger than the love of freedom’ (Hayek, 1944 p.95). These points directly relate to Lyon’s observations of the need to give up some of our privacy in order to participate in society. It may be that in many instances, the fear of being left behind by society or to be reduced to its fringes may be something that the majority
ould prefer to avoid. This may be due to the many perceived benefits of participation
at greatly outweigh the disadvantages of a loss of some freedom. On the other hand,
re dangers associated with not being accepted or part of the society in which we live,
at of rejection and possible destitution is a situation that most would find unacceptable
ad to be actively avoided.

he use of surveillance technologies such as CCTV is therefore accepted not only as a
means to the prevention and detection of crime but is also accepted as inevitable now
hat it is in place. The fact that there was little consultation or information available to
be public about the potential for abuse, and a lack of concern that the initial uses would
ad to a proliferation of such systems is now seen as largely irrelevant. This is due to
s physical presence and public familiarity with it combined with the difficulty of
moving such systems once in place. However, surveillance is not the only privacy
concern here. The inappropriate use of information, access to personal data by
authorised persons, and the use of personal data without the permission of the
individual can all be seen as invasions of privacy (Introna and Pouloudi, 1999). This is
articularly the case where the individual does not have the ability to maintain control
ver personal information (Clarke, 1987). Privacy threats can occur where access is
en as appropriate but the extent of the information gathering goes beyond that
plicitly required, an area of concern that the Data Protection Act 1998 is intended to
dress. Although surveillance and infringement of privacy are not synonymous, the
of surveillance may facilitate the occurrence of privacy invasion.

ne may never actually know what kind of data is being held, where, by whom or for
hat purpose. Authors such as Lyon (2001), Clarke (1999, 1994, 1987) and Introna
identify the potential threats of the use or over-use of available
technologies for surveillance purposes. Their work indicates that present information
technologies have a huge potential to invade privacy. It is clear however, that it is not
just the technology that is in need of study, but also the uses to which it may be put, and
the motives of those who would use it.

1.17. Privacy and Transparency

Having nothing to hide, suggests that disclosure of information would be of little
concern. This suggestion is often used to excuse privacy invasion. However, that one
may have nothing to hide does not alter the fact that any invasion into an individual's
freedom without informed consent can be seen as an infringement of civil liberties. This
suggests that there is some urgency to ensure privacy protection for the individual so
that for example; going to the bathroom may be conducted in private and with dignity.

Future developments in society may mean that what is acceptable now may be less so in
the future. This may lead to persecution. An example may be the problems
encountered by homosexuals in a society, which becomes homophobic due to the fear
of AIDS. In this case, previous transparency of information may lead to the
identication of homosexuals and their subsequent persecution. Further, the release of
personal information may be inappropriate due to the fear of crime. An example of this
where a disabled person feels that they have nothing to hide about being disabled, but
may still be afraid to reveal this on the world wide web for fear that criminals will
access that information and use it to rob them.
here may be some areas in which transparency is seen as necessary. The ability of
agencies providing child care to examine the criminal records of potential employees to
ensure that those who committed offences against children are rejected is a clear
example of where transparency of information is essential. However, it does not mean
that there is an equal requirement for all of society to operate under such scrutiny at all
times. The same person rejected as a possible child care worker should not have to
reveal their past, however unsavoury in order to obtain a bank account. However,
someone convicted of fraud may be expected to do so. The extent of transparency
should therefore, depend on the situation at the time. However, the feelings and
sensitivities of the individual may indicate a need for greater or lesser privacy
de pending on the individual’s perceptions.

Each individual has a different idea as to what is and is not acceptable to reveal. Much
depend on how much privacy that the individual has come to expect in their lives.

Someone who has chosen a path that leads to fame and celebrity cannot expect some
pects of their lives to be free from the scrutiny of the media. However, where media
interest goes beyond genuine ‘public interest’ and into the realms of ‘mud slinging’ and
personal attack the privacy, of any individual, no matter how famous, should be
maintained.

Applicants for change as in the case of gun control after the loss of a loved one may
expect to maintain a greater degree of privacy in their personal lives than a celebrity on
the path to fame and fortune. This may be due to the very nature of their media seeking.
The difference is, between those seeking self-advancement through the manipulation of
the media, and those campaigning for public awareness and change due to some tragic
vent. This suggests that the personal motivation for media attention may have an impact on the degree of privacy that can be expected. Therefore, those seeking to benefit society may be entitled to a greater degree of privacy protection than those seeking self-fulfillment and career progression.

The point at which the individual is able to erect boundaries is not clear. What is clear however is that boundaries may move according to the individual’s circumstances at any given time? However, there is a need for some control of personal information in order to prevent individual lives becoming mere commodities. Furthermore, low levels of protection required at one time should not undermine the amount needed at another me. As Berlin states, ‘a frontier must be drawn between the area of private life and that of public authority’ (Berlin, 1969 p.124) and that ‘some portion of human existence must remain independent’ (Berlin, 1969 p.126). The subjective nature of privacy and the changing perceptions of individuals mean that privacy protection will always be difficult and subject to contextual interpretation. Research that uncovers individual perceptions and trends of attitude towards privacy is therefore critical to aid in the future decision making process.


Social psychology is ‘an attempt to understand how the thoughts, feelings, and behaviour of individuals are influenced by the actual, imagined or implied presence of others’ (Allport, 1954 p.3). To discover the feelings, awareness, sense of importance and behaviour of the participants concerning the issues of individual and organisational privacy were to be discovered through case study interviews were conducted (see
Further, by the adoption of interpretive interactionism as an analytical tool it is possible to discover the perceptions of individuals from their lived experiences (see chapter 3).

Social psychology is chiefly concerned with the analysis of the behaviour of individuals and groups in their social interactions, particularly where it relates to the influences on behaviour, norms, compliance with rules and interactions. With regard to privacy within organisations, and particularly the image being presented by the individuals within it, a social psychological perspective enables some insight to be gained into the reasons, feelings and motivations of the individuals combined with the effects of organisational culture on those perceptions.

Social psychology however, has largely ignored the issue of privacy within its realms and 'there continues to be relative indifference to privacy, as a theoretical or research interest, among psychologists in general' (Margulis 2003a p.243), which in view of the apparent need for privacy as an essential element of dignity, self esteem and autonomy (Fried, 1968), is a rather surprising finding in that privacy appears to be important across a range of behavioural areas, societies, and species' (Margulis, 2003a p.257)

In view of this, the issues of privacy within social psychology as related to this thesis have been examined from a largely fresh perspective, drawing directly from the main body of work into the behaviour of individuals and groups from psychological and social psychological perspectives. This section therefore does not intend to re-evaluate the issues of privacy from within the discipline of social psychology per se, but to
consider its findings as a signpost towards the understanding of privacy perceptions as revealed by the individuals in the case studies, whereby 'a proper understanding of psychological aspects of privacy must include the interplay of people, their social world, the physical environment, and the temporal nature of social phenomena' (Altman, 1990).

When considering the role of the self, and the impact that privacy or its lack may have on the way that the individual portrays themselves to the world, Goffman (1990) in his seminal work *The Presentation of Self in Everyday Life*, introduces several key concepts that are critical to the analysis of the individual, and which relate directly to how individuals perceive themselves and their role in society. Individuals live in 'a potentially infinite cycle of concealment, discovery, false revelation and rediscovery' (Goffman, 1990, p.20). How we present ourselves to the world therefore is seen to be a performance, whereby different 'masks' are presented to the world depending on the role that is being played at the time. In order for this role to have validity and to be convincing to the observer, it is necessary for the actor to have 'belief in the part one is saying' (Goffman, 1990 p.28). Moreover, individuals may present a 'self' that is not necessarily 'true' but is regarded to be true both by the performer and by the audience.

From the perspective of privacy analysis within the organisations studied, this means that individuals who are part of the organisation and those who come into contact with it should be convinced in a reasonably rational way that its privacy policies and practices dictated by its members are 'good enough' for the needs of the participants, whether or not this is actually true or offers a misrepresentation of the truth. The presentation of appearances therefore is as important as the actual 'truth' being presented. Further 'if
The principle ideal aims of an organisation are to be achieved, it will be necessary at times to by-pass momentarily other ideals of the organisation...while maintaining the impression that these other ideals are still in force’ (Goffman, 1990 p.54).

The maintenance of appearance will also be based on the influence of its individual arts and their beliefs because ‘cultures are not free-floating entities, but are in most of their aspects embodied in the social structure and the behavioural patterns of the people’ (Fahoda 1978, p.77). These behavioural patterns and subsequently the culture of the organisation that is presented both internally and externally will therefore mutually shape and be shaped by the beliefs and perceptions of the individuals within it.

Even whilst there are external influences such as government directives and statutes, the interpretation of such rules and regulations will be largely dependant on the culture of the organisation and the related behaviours of the individuals and groups operating within it. In this way, individuals may present their beliefs of privacy issues from a personal perspective that is closely correlated to that of the organisation within which they are a part, in that there is a ‘strong tendency for groups of people to share the same beliefs, personal knowledge and meaning about referents (objects and events) that are significant to their referent group’ (Harvey, 1997 p.147)

How individuals construct meaning and beliefs therefore is largely, but not wholly, influenced by their membership of groups and their role within them. This means that though some fundamental themes of agreement may be apparent throughout an organisation, there will still be subtleties and in some cases quite striking differences in beliefs or perceptions of individuals within it and ‘while different thoughts and
beliefs may share many or most of the same characteristics, difference on only two or
are critical criteria may produce patterns that are qualitatively different from all the
other systems or patterns’ (Harvey 1997, p.159). It is from this perspective therefore
that the analysis of the perceptions of those individuals within the organisations selected
for in-depth study was undertaken and which is detailed in chapter 5 section

4.2. Definition of Terms

Throughout this chapter, there has been much description and analysis of the nature of
ICTs and Privacy. This has involved definitions, descriptions and analysis of what
privacy means to individuals, society and organisations. We have considered how
legislation impacts and is impacted by privacy concerns, and how technology and its
devancement may affect perceptions of privacy. There has also been considerable
analysis of the nature of privacy from different philosophical perspectives. Its
relationship to liberty and freedom has been examined and how technological society
needs privacy for individuals to perpetuate innovation, and maintain well-being.
However, certain terms have been used throughout that require clarification. This is
because often they are used in such diverse and subtle ways that a definitive explanation
of their use within the context of this thesis is required. The following section will seek
not only to define these terms but also to analyse their nature from a philosophical,
sociological and practical perspective in order to clarify their meaning within this work.

4.2.1. Perception

76
perception is a word that requires definition for this thesis, as much of the questioning is
do discover individual perceptions of privacy and the influence of ICTs on those
perceptions.

The noun ‘perception’ is described as ‘the act or power of perceiving; discernment;
prehension of any modification of consciousness; the combining of sensations into a
recognition of an object; direct recognition; a percept; reception of stimulus’ (Chambers
dictionary, 1999). Further, the root of the word ‘perceive’ is defined in the Oxford
english Dictionary (1989) as ‘to apprehend with the mind; to become aware or
conscious of; to observe, understand’. However, these definitions alone are insufficient
to explain what is meant by perception for the purposes of this thesis.

Within the field of cognitive psychology, perception is concerned with how individuals
see, feel and experience stimuli, ‘those processes of acquiring and utilizing information,
which enable us to make sense of and interact with the environment’ (Roth, 1981 p.10).
According to Velmans (1999) ‘Perception becomes conscious at a late-arising stage of
spatial-attentive processing concerned with information integration and dissemination’
Velmans, 1999 p.01). In other words, perception can be described as the way we take
information, how we process it and use it in the context of our surroundings (Merikle
and Daneman, 1998).

However, not only is it important to obtain clarification of perception using psychology
as a basis for definition, it is also important to view perception from the view of
philosophy.
Philosophy, which is concerned with the mental aspect, endeavours to separate out whatever in our knowledge and ideas is due to the effects of the material world, in order to determine the nature of pure mental activity. The natural sciences, on the other hand, seek to separate out definitions, systems of symbols, patterns of representation, and hypotheses, in order to study the remainder, which pertains to the world of reality whose laws they seek, in a pure form.

Helmholtz (1878, p.1).

A philosophy, perception can be defined as the method of obtaining information about our surrounding world, through our senses, and then to understand and interpret this information as beliefs. Initially, this may appear to be a way of interpreting the concept of perception. However, there are other factors, which must be considered, which do not allow for such a simple explanation of perception. Firstly, it is possible that our perceptions are incorrect and that our interpretation of the world is based on misinformation. Secondly, we can suffer from illusion, hallucination or fantasy, and thirdly, it is unclear how much we can truly believe in what we perceive and therefore the concept of validity is brought into question. (Internet Encyclopaedia of Philosophy, 001)

To answer those problems of definition, by identifying and validating the arguments for perception as a concept, and to counter the possibility of incorrect interpretation, misinformation, and illusion, would involve delving deeply into the realms of

While this description may be controversial, it does illustrate a viewpoint that is worth further consideration here, and the controversy about the nature of philosophy is outside the scope of this thesis.
philosophy and cognitive psychology. However, the nature of this study means that to do so would significantly go beyond the scope of this research.

The above examination of both philosophical and psychological viewpoints, has clarified what perception is at a basic level. Even without resorting to in-depth psychological or philosophical analysis to discover what perception is, it is possible to consider that perception is how we see the world based on the stimuli we receive and our interpretation of those stimuli. This provides an explanation of perception that is sufficient for this study.

2.2. Organisation

This thesis is not seeking to examine organisational theory, but to consider privacy perceptions from the perspective of the individuals within the organisations. However, there is still a need to identify and define the meaning of the organisation within this work. In the context of this thesis; an organisation is taken to mean a body or group, within which individuals work and which whilst having no consciousness itself, does create an ethos or consciousness within it, and which is created by those who manage and implement those policies. The organisation performs its function either within the public sector or private sector by the individuals within it operating certain tasks to the best of their ability. Therefore, the organisation can be seen as a machine with the individuals within it operating as the internal workings of that machine.

2.3. Individual
he individual is probably the most important entity in this research. The concept of
the individual and its history has been explored in Chapter 2. However, for the
purposes of definition, the individual is that autonomous element which is subject to the
influences of both organisations and society, but which is capable of free
thought and free will, and who can make judgements based on their own predilections,
references and morality.

The individual has free will, personal autonomy and has a persona that reflects its
organisation but which also reflects its own personal life. It is also influenced and
adapts to its environment and can have several different viewpoints simultaneously
(Young, 1986). The individual where it is considered to be a human being is not
restricted to previous held beliefs and can change their opinions and beliefs at any time.

Therefore, the individual for this thesis is an organic, autonomous being with
exceptions and perspectives that are subject to change and alteration, but which
an influence and be influenced by external factors in similar ways to that of the
organisation.

2.4. ICT

Information and Communication Technologies (ICTs) are not purely concerned with
computers but can be associated with any form of technique or tool that enables the
production and distribution of information. In this thesis however, the term ICT is
predominantly used to indicate the use of the computing and telephony technologies
that were developed during the latter half of the twentieth century. The impact on
privacy perception that these technologies engender is fundamental to the concepts
eing explored in this thesis. Future developments may create further privacy concerns and erosions and yet the use of such technologies if used effectively and ethically, may actually bring about greater freedom, participation and efficiency. The need for study of the impact of ICTs on individuals and organisations cannot be overstated.

2.5 Culture and Ethos

Within this thesis the terms culture or ethos appears on a regular basis. For the purposes of this work the two words should be considered as meaning the norms and traditions of the environment in which one finds oneself.

2.6. Rights

Here are several approaches to the concept of a right that are considered within western philosophy (Mishler, 1991; Melden, 1977). The areas of legal rights, human rights and moral rights are the subjects of great philosophical discussion (Cranston, 1973). However, this thesis does not intend to explore the concept of rights per se, but examines the right to privacy from the perspectives of the participants in this study. For the purposes of this thesis therefore, where a 'right' is referred to, it is taken to mean the expectation and belief that there is a moral and universal obligation to ensure that right is guaranteed and protected, which in this instance is chiefly concerned with the right to privacy.

3 Conclusion

This chapter has examined the historical development of privacy and the individual and e effects of technology on societal development and needs. It has established that
Privacy has become essential in the modern technological world and that it must be protected. However, the need to protect citizens from criminals and terrorism means that some privacy may need to be relinquished on occasion. It is important therefore that the privacy perceptions of individuals are discovered to enable policy decisions to reflect attitudes and to discover the extent of privacy protection expected. Privacy is being eroded by the introduction of policies and legislation which may be reactive in nature and this work suggests that there must be a balance between privacy and security that needs to be considered at all policy levels. The nature of privacy and the impact of its combined with a discussion of the potential for privacy invasion from commercial as well as public sector bodies indicates a need for awareness raising and education to low informed choices to be made.

His research considers the growth of technology and the effect this has had on individual perceptions of privacy within both a public and private sector organisation. The above chapter represents a summary of concepts and ideas that are currently being considered in the area of privacy, technology theory and practice. The following chapters detail the methods, tools, analysis and findings of this research. It considers tensions between individual perceptions, those of the organisations in which they work, the policy makers who decide the extent that privacy should be protected and who formulate legislation to reflect this.
Chapter 3: HERMENEUTICS AND INTERPRETIVE INTERACTIONISM: QUALITATIVE APPROACHES TO EMPIRICAL ENQUIRY.

In order to answer the research questions set out in chapter 1 it was necessary to decide on the approach to the whole project. It was clear from the outset that a positivist approach was unsuitable for the type of questions being asked. Firstly there was an extensive consideration of fundamental and theoretical perspectives on research and only those aspects of direct relevance are reported within this thesis. This work required an intuitive approach in order to delve into the largely subjective area of individual perception. To gain such insight, the use of interviews was the obvious choice requiring the researcher to listen to and analyse the dialogue. Further, it was necessary to contextualise the information by considering the internal culture of the organisation and the role of the media in shaping perceptions of privacy.

1. Consideration of Research Approaches

The critique below gives an account of the approaches and techniques utilised for this research. Other methods of enquiry were considered and rejected as being unsuited to the study (Granger, Fischhoff, Bostrom and Atman, 2002; Myers, 2000). Firstly there was extensive consideration of fundamental and theoretical perspectives on research. Therefore both qualitative and quantitative approaches were considered (Cresswell, 1998; Denscombe, 1998; Denzin and Lincoln, 1998; Miller and Dingwall, 1997; Morse, 1994; Silverman, 1993). The uses of quantitative, positivistic techniques such as
statistical analysis, testing, and formal questionnaires were considered (Galliers, 1992; Sauman, 1992).

As the hallmarks of quantitative work are numbers, statistics and the use of equations, a positivist stance is often taken during quantitative research. Positivist research may be seen as a form of inquiry in which 'only those statements which are reducible to elementary (or 'atomic') statements of experience' (Popper, 1959 p.35) are considered scientifically legitimate. This means that according to positivism, each piece of information must be reducible to a code, number or standardised text that can then be measured and categorized (Comte, 1957). In this way positivism has been described as a stance which 'postulates that the universe comprises objectively given, immutable objects and structures' (Hirschheim, 1985 p.28), and that 'these exist as empirical entities, on their own, independent of the observer's appreciation of them' (Hirschheim, 1985 p.28). Positivist or detached research is therefore suited for research where the variables are subject to reductionism and measurement.

- It claims to be always objective.
- The observer is required to be separated from the observed.
- The results are universally generalisable.
- There is a distinct and observable cause and effect.
- There are no values placed on the information beyond the observable results.
Positivist social science research involves independence, enabling a choice of what to study based on objective criteria. Easterby-Smith, Thorpe, and Lowe (1991 p.24) however reject this and claim that

... the task of the social scientist should not be to gather facts and measure how often certain patterns occur, but to appreciate the different constructions and meanings that people place upon their experience. One should therefore try to understand and explain why people have different experiences, rather than search for external causes and fundamental laws to explain their behaviour.

To enable perceptions to be revealed without the constraints of structure, it was necessary to develop a level of trust and openness that enabled the participant to discuss the issues freely. The formality of structured interviewing would have precluded the ability of the participants to elaborate on the questions asked. The development of trust and openness within the interviewer/interviewee relationship meant that the maintenance of neutrality and separation would be impossible. Therefore,

Where there is a need to discover feelings, hopes, thoughts and fears from individual human subjects who may be influenced in many different and unpredictable ways, it may be neither possible nor desirable to factor out those outside influences' (Denzin, 1989 p.27-28).

Moreover, the uniqueness of individuals and interpretation of circumstances can lead to different responses to the same experiences. Studies requiring generalisable results orne out of the categorisation and codification of the human experience may have reater expectations of standardisation than qualitative studies. A positivistic approach therefore was not appropriate for a study seeking individual perceptions and which
intended to discover feelings and nuances regarding the issues requiring considerable flexibility in data collection and analysis.

Whilst positivist approaches are scientifically rigorous, there are concerns that human social behaviour may not be sufficiently regular and predictable to be amenable to positivist research. Similarly, ‘the ‘positivists’ position failed to appreciate the fundamental experience of life in favour of physical and mental regularities’ (Galliers, 1992 p.43). In this case, structured and rigid techniques that do not consider the richness of the context in which the research is placed may be unable to provide the flexibility of approach and practice needed. This is particularly problematic where individuals are concerned and where conclusions may not be reducible to quantifiable data points. Where a positivist stance is taken therefore, ‘the flesh and bones of the everyday life world is removed from the substance of the research itself, thereby diminishing the usefulness of the research for subsequent investigations’ (Feagin, Drum, and Sjoberg, 1991 p.7).

A good example of the problems of statistical or positivist approaches in predicting or analysing human behaviour is the 1992 UK election results. This predicted a Labour lead of 0.8% which should have resulted in a hung Parliament. The final outcome of the election was that the Conservatives were found to be 7.5% ahead with an overall majority of 21 seats (Alba Org, 2003 p.1). This failure of quantitative techniques and statistical analysis does however raise questions of interest to qualitative researchers who could further investigate the reasons for this result through in-depth study of individuals or cases. Quantitative work may generate hypotheses interesting to qualitative researchers. Similarly qualitative work may discover such veins of potential
hypotheses, which can then be measured by quantitative work and may create opportunities for further research.

The qualitative approach to research is concerned with an interpretation of meaning 'to determine what an experience means for the persons who have had the experience and are able to provide a comprehensive description of it' (Moostakas, 1994 p.13). The aim of the research was to discover feelings about the phenomena at the time of the study, from the perspectives of those directly involved, within the context of their experiences. By using qualitative, intuitive methods, this research was able to discover and distinguish more subtleties of feelings and perceptions than would have been discovered and considered relevant within a quantitative/positivist study.

Consideration of qualitative tools was the next decision to be made once quantitative inquiry was rejected for this study. There are several different data collection tools that were researched including ethnographic observation, action research, and case study (Stake, 1994; Yin 1994; Easterby-Smith et al, 1991; Denzin, 1989, 1984, Van Maanen, 1983).

Significant consideration was given to grounded theory as a complete methodology for approach, data collection and analysis (McCarthy, 1999; Strauss and Corbin, 1997, 1990; Glaser, 1992, 1978; Glaser and Strauss, 1966). Grounded theory attempts to generate a theory as the research progresses and as the data are analysed, resulting in the identification of a theory. In this way at the end of the study one 'should simply code and analyse categories and properties with theoretical codes which will emerge and generate their complex theory of a complex world' (Glaser, 1992 p.71). This is an
ttempt to discover how people act. Grounded theory is defined by ‘its insistence, from the start, on generating abstract conceptual categories to account for the data being studied’ (Punch, 1998 p.211).

Grounded theory is intuitive and close to the data, enabling themes to be tested as patterns emerge (Easterby-Smith et al, 1991). In many respects this methodology would have been suitable for this research, however, the fundamental requirement that the researcher continually return to the source of data to collect further information in order to achieve saturation was not achievable for this work. This was due to an inability to return to the case study organisations beyond the two-phase interview process agreed with the management at the outset. The selection of analytical techniques was also considered in great depth involving the study of several before the final decision was made (Madill, Jordan and Shirley, 2000; Hood, 1998; Denzin, 1989).

1.2. Hermeneutics: Description and Understanding.

After careful consideration of the above techniques, approaches and methodologies, a hermeneutic approach to the research was selected and is described below. Case studies were conducted to collect the data, and the data analysed by utilising the tools of Interpretive Interactionism (Denzin, 1989).

The decision to use a hermeneutic approach to the entire project was grounded in the need to discover meaning in context rather than a desire for quantifiable results. The principles of the approach are identified by key authors in the field such as Gadamer and Heidegger. Hermeneutics is ‘the science of interpretation, esp. of Scriptural exegesis; the study of human beings in society (philos)’ (Chambers Dictionary, 1999).
The word is derived from ‘Hermes’, the herald of the Greek gods. As the messenger of the gods, Hermes was required to interpret what was said so that humans could understand what the gods required of them. It is easy therefore, to understand how the concept of hermeneutic enquiry developed from these roots into the interpretation of meaning through discovery of the underlying message.

Hermeneutics has been used as a philosophy of analytical interpretation since the 16\textsuperscript{th} century. It was originally developed and validated by its use in the translation and interpretation of biblical texts. The idea was that the translator/interpreter would attempt to submerge themselves into the psyche of the original authors. In this way, the approach enabled an interpretation to be made within the context of the author’s experiences and intended meaning by ‘entering the mind of the author of a text, to understand him better than he understood himself’ (Musgrave, 2000 p.10).

His approach stresses the discovery of the objective meaning of what is being said, by interpretation and intuitive reflection on the whole, its context, dialogue, tones and reflections. The dialectic is seen as crucial in hermeneutic research and several types of dialectic are needed during the process of understanding. Butler indicates that what this requires, is a Socratic question and answer dialectic. This involves the pre-understanding of Hegel and Aristotelian deconstruction of the text in order to arrive at a true understanding (Butler, 1998 p.290).

The use of a hermeneutic approach in social science research has been aided in its development and interpretation by thinkers, including Husserl, Heidegger and Gadamer. Husserl’s approach was largely philosophical, requiring that ‘The man, as an entity
which belongs to nature and as a person related to other persons, to a ‘society’, is swept way by the broom of *epoche* together with other ‘impurities’ (Husserl, quoted in auman, 1978 p.120). Husserl’s early theories on truth however failed as he did not consider the validity of perception where there was a need to ground individuals in the context of their experiences. If one was to completely remove influences such as culture, society and ‘man’ there would be nothing left to re-engage. Whilst valid for philosophical enquiry, this study required greater reflection of perception within the specific area of privacy and computer use. Therefore, an approach to hermeneutic inquiry, which challenges Husserl’s view as unreal and unusable, was considered more appropriate.

Heidegger’s view ‘understanding is a mode of being, rather than a mode of knowledge’ (Bauman, 1992 p.148). This led to a theory of hermeneutic understanding that embraces the influences that are inevitable by the act of ‘being in the world’. This complements the aims of this work by considering context as being critical to an understanding of meaning. Bauman (1992) similarly considers the Heideggerian view of hermeneutic enquiry in that knowledge is ontological, (examination of ‘nature’ or being’) rather than epistemological (scientific acquisition of knowledge). Therefore, when a hermeneutic approach is viewed from a Heideggerian perspective, it accepts the need to consider contextual influences to discover its ‘essence’ or ‘nature’.

Moreover, Gadamer states that ‘Hermeneutics is an art and not a mechanical process’ (Gadamer, 1989 p.191, emphasis in original). This offers a complementary stance, and enhances the approach taken by Heidegger, allowing for some of the philosophical ideas suggested by Husserl. Gadamer’s approach allows for contextual enquiry along the
nes of Heidegger but remains within the intuitive perspective of Husserl. If one rejects the importance of the self as required by Husserl, we also reject the concept of the power of prejudice which in unachievable as ‘every researcher brings preconceptions and interpretations to the problem being studied’ (Heidegger, quoted in Gadamer, 1975.232).

This power, which is brought to the research by the researcher through their own cultural and social experiences, expectations and, to use a Heideggerian term; ‘preunderstanding’, cannot fail to influence the interpretation of the data. The researcher can, by indicating an awareness of this potential, and using their pre judgement of the situation in a critical manner, help ‘to distinguish between legitimate and illegitimate prejudice’ (Butler, 1998 p.288).

Gadamer considers that it is the task of the researcher to interpret text, based on an understanding of the language or dialectic used. One of the key principles of Gadamerian hermeneutics is the movement away from ocularcentrism i.e. that which is determined by what is ‘seen’ or perceived (Warnke, 1987). The reason for his loss of faith in the visual as a valid form of interpretation is that the visual can be illusionary or superficial. An illustration is to liken ocular centrism to the study of a painting by a literal examination of a picture. Whilst this is one element of understanding, it is not helpful in interpreting the artist’s intention when producing the painting, nor the meaning that the artist was trying to portray within it. The art of hermeneutics from a Gadamerian perspective is therefore to not only look at the superficial and visual within a text, but to investigate the parts of the text which make up the whole. The
The investigator should therefore consider the effects that cultural and social influences may have on the interpretation and meaning and thus to arrive at a ‘fusion of horizons’.

The above discussion develops the argument for a combined approach referring chiefly to the works of Gadamer and Heidegger. Hermeneutic enquiry requires an analysis of the data in context, not only from its origins, but also from the perspective of the researcher so that, ‘the meaning of the part can be discovered only from the context’ (Gadamer, 1989 p.190). There is a perception in their work that the investigator needs to be aware of the social and cultural context in which the research is conducted, along with an awareness of the researcher’s role in the enquiry to consider ‘the primacy of human thought and existence within historical, communal, and cultural contexts.’ (Butler, 1998 p.287)

The influences of tradition and culture and many other seemingly conflicting or tempestuous factors are therefore, routes to achieving understanding. Heidegger argues that this is the ‘quiet authority of das Man’ (quoted in Butler, 1998 p.287). This can be explained as the reassuring realm of ‘the people’, or the ‘them’. Once understood, and that perspective achieved, it is then possible to verify or refute the influences of culture and so forth on the discovery of knowledge as truth. ‘The ‘fusion of horizons’ is therefore the culmination of the act of understanding between interpreter and interpreted, between researcher and researched’ (Butler, 1998 p.289).

In this way, the examination of each component part to reach an understanding is necessarily combined with an awareness of the investigator’s pre-understanding. This must therefore be examined as understanding develops. Each time an understanding is
A new prejudice is born and the process of understanding, allowing for the new prejudice begins, thus the perpetual 'circle of understanding'. However, how do we arrive at a conclusion if the circle is perpetual?

There are two realms that determine the existence of an object of enquiry within hermeneutic theory, which explains how the researcher may achieve knowledge using his approach. In this respect the key to understanding is consideration of how the actors perceive the object of enquiry. Within the realm of existence, an object can be 'ready-to-hand' (zuhanden) in that they are so familiar as to require no examination or critical evaluation, or 'present-at-hand' (vorhanden). This status of 'present-at-hand' is where an object or phenomenon is or has become (due to new developments or influences) unfamiliar, and any preconceived ideas as to its purpose or meaning has either changed or requires interpretation. This position of 'present-at-hand' provides the starting point for enquiry. The study then envelops the concept of pre-understanding and the nature of awareness of the potential for illegitimate interpretation. Therefore, by being aware of the concepts of zuhanden and vorhanden, the researcher can set about the rejection of illegitimate interpretation and achieve a greater legitimacy of understanding of the phenomena (Gadamer, 1989).

By working through the circle of understanding, and as the phenomenon being investigated becomes more exposed, there will become a point where vorhanden becomes zuhanden and the phenomenon is considered 'known'. However, 'known' phenomena are subject to future influences and challenges, which may require further analysis. Such analysis is likely to be undertaken as a result of further study.
The above analysis clearly indicates the necessity to use a hermeneutic approach, which
rejects the relatively ethereal stand of Husserl in favour of the more practical
approaches of Heidegger and Gadamer. This will ensure that the nature of the data will be fully appreciated in its analysis. Hermeneutics focuses on interpretation of meaning to discover what is being said and what is meant by what is said, during interview, at transcription or during the process of reading those transcripts. The researcher hears the 'voice' of the individual and interprets what is said. The meaning of the text can therefore be discovered through intuitive interpretation allowing for the cultural context in which it is derived.

Articulation in the world by the researcher cannot be factored out of the analysis. In order to develop a meaningful interpretation of a situation, the researcher must be immersed into the phenomenon. This provides a 'slice' of understanding where 'an understanding and interpretation of everyday life must consider the gendered, situated, structural, and practical features of that world' (Denzin, 1989 p.27). Description rich, interpretive analysis does not attempt to generalise but to understand perceptions and interpretations. The purpose of this approach therefore is to provide a snap-shot of a phenomenon that is a detailed, rigorous and meaningful observation. In this way 'the process of interpretation is shaped by history, power, emotionality, and beliefs concerning knowledge' (Denzin, 1989 p.28). To discover perceptions and to answer the research questions detailed in chapter one required an intuitive and interpretive study to be undertaken. A hermeneutic approach therefore was considered appropriate for this work.

3. Interpretive Interactionism
The next step towards achieving a framework for the research was to decide upon the data collection and analysis tools that would best utilise the principles of hermeneutics whilst also providing a clearly defined mode of operation. Due to the intuitive nature of the approach, Grounded Theory (Strauss and Corbin, 1990) was considered and later rejected in favour of an adaptation of the tools of Denzin's (1989) interpretive interactionism. These tools consist of deconstruction, capture, bracketing (reduction) the identification of the epiphany (transformational experiences), construction and contextualisation and are detailed in section 3.6 below.

Denzin developed the chosen method for this study in 1989. At this time he was undertaking work with recovering alcoholics at Alcoholics Anonymous meetings and was looking for a method that would examine their life experiences in an intuitive manner.

Denzin sees his work as considering existentialism and interactive analysis of text by the use of Sartre's (1958) progressive-regressive method of analysis. This enabled the development of a 'critical-interpretive method' which 'seeks to situate and understand a particular class of subjects within a given historical moment' (Denzin, 1989 p.21).

In close examination of Denzin's techniques it became clear that his approach implemented both hermeneutical enquiry and research into individual perceptions.

Interpretive interactionism is an 'attempt to develop interpretations grounded in the worlds of lived experience' (Denzin, 1989 p.167), and is an appropriate method to aid in the discovery of the perceptions of individuals. This is particularly so where the intent
of the research is to gain knowledge of the experience of being within the organisations studied.

Interpretive interactionism has its roots in symbolic interactionism and the largely unpublished work of George Herbert Mead (Harris, 2003; Nelson, 1998; Natanson, 1973). Symbolic interactionism uses symbols to describe and interpret the interactions and impact of social situations on people within the context of the phenomenon being researched. It was developed initially by his student Herbert Blumer after Mead’s death. Blumer described symbolic interactionism as ‘a down-to-earth approach to the scientific study of human group life and human conducts’ (Harris, 2003 p.1). Its influences are based in the philosophy of pragmatism, the perspectives of Charles Darwin and the ideas of social behaviourism.

Symbolic interactionism and interpretive interactionism both consider the importance of trying to discover meaning from a socially interactive phenomenon. How people interact in social settings are seen as first indicators for the discovery of meaning. The scope and nature of that influence is further dependant on the circumstances in which we find ourselves, and that ‘human beings – whatever else they may bring to a situation are influenced by what goes on in that situation’ (Charon, 2001 p.22), and are therefore context specific. Where people interact in order to ascribe meaning to an activity, ‘the individual engaged in interaction with another must be able to assign meaning to the acts of the other in such a way that he or she can act appropriately’ (Euwitt, 2003 p.53).
y understanding the meaning of interaction the influence of relationships on understanding of a phenomenon can be discovered. This awareness allows the researcher to account for that influence in the analysis.

In this way, the perspective of social interaction also considers the thoughts that accompany the act of being within a phenomenon. By considering the phenomena from within, as part of it, perspectives can be drawn by the researcher from the experience. This enables the researcher to be immersed in the phenomena under study, and yet be aware of their immersion at the same time. This allows a greater depth of understanding to be achieved and enables the researcher to focus on 'how people define their world and how that definition shapes their action' (Charon, 2001 p.229).

The social interaction elements of symbolic interactionism are revisited in Denzin's approach particularly by the need to discover the 'lived experiences' within the social phenomena being researched. Further, ascribing meaning from within the context of the phenomena is hermeneutic in its approach.

Where interpretive interactionism departs from symbolic interactionism is the focus on ascribing and understanding symbols that are used by the subjects to describe the phenomena thus increasing the level of understanding of the whole phenomena. Symbols may be words, phrases or reactions that are familiar to the subjects and which universally describe responses to and interpretation of the phenomena, within its own context.
enzin however, utilises the techniques of interpretive interactionism to research and
considers less the prescribed symbols of cognitive psychology and more an intuitive and
interpretive understanding of hermeneutic research.

Defining a phenomenon within the tenets of both symbolic and interpretive
interactionism requires an on-going process of analysis. The understanding of a
phenomenon develops as the research process delves deeper and the analysis is
conducted. As further information is discovered and the phenomenon becomes ‘known’
as expected when using a hermeneutic approach) then it becomes possible to define
and to gain meaning of the lived experiences of the research subjects.

As previously discussed in section 3.2, hermeneutics is a thematic approach to
understanding that focuses on interpretation, and is aware of the role of the researcher in
reporting the research findings in that ‘value free interpretive research is impossible’
Heidegger in Gadamer, 1989 p.232). Hermeneutics can be seen as a philosophy of
search in that these and other methodologies such as grounded theory (Glazer, 1992;
Raus and Corbin, 1990) are influenced or have their roots in its basic principles.

Using these approaches and techniques it is possible to gain insight into the world of
lived experiences and make it directly accessible to the reader. Interpretive
interactionism therefore uses tools, which endeavours to capture the voices, emotions,
and actions of those studied by interpreting the interactions of actors in social situations,
using their own words and from their own lived experiences.
Denzin initially stressed that his approach should only be used to examine personal troubles and the public policies set out to alleviate those problems. However, this method can be easily utilised in the examination of perceptions in other areas of research. Denzin later acknowledges that 'the focus of interpretive research is on those life experiences that radically alter and shape the meanings...given to themselves and their experiences' (Denzin, 1989 p.10). This does not indicate that 'troubles’ per se are the only qualifying factor in the use of interpretive interactionism. Instead, a life hanging experience or one that has a considerable impact may be considered as a focus or research using the techniques of interpretive interactionism. For this research the introduction and implementation of computing technologies can be said to have had such an impact.

Further, there is no universal law that states that a method cannot be used in an alternative context. In this study, the use of this method was seen to be appropriate due to the interpretive nature of the research project, and the strength of Denzin’s method to interpret the information gathered to produce interesting, valid and useful results. It could almost be said that despite his initial caveat on its use, that his method is tailor made for this research.

Further, his approach has been used and developed in other contexts as illustrated by heehan (2000) where this approach was used in the analysis for his doctoral thesis entitled 'Learning and Implementing group process facilitation: Individual experiences'. His focus on the individual and their experiences was particularly relevant to this current research.
Denzin offers a definition of his method, which further clarifies its validity for this research. Interpretive interactionism is ‘That point of view that confers meaning on problematic symbolic interaction’ (Denzin, 1989 p.13). In interpreting his definition for the purposes of this research, interpretive interactionism therefore can be considered to embrace the interpretation of individual perceptions of areas of experience that may be problematic or challenging.

Denzin identifies his method and its application in several ways:

- To identify different definitions of a problem. – Denzin uses the example of battered wives and their interpretation of facilities offered and how they are used, compared with how the providers perceive the provision of the facilities. This example clearly mirrors the research undertaken here in that the identification of the problem in this case is that of the use of computerisation and its impact on perceptions of privacy in the lives of the interview subjects. This is then considered in light of how the organisations they are part of have facilitated the use of computing technologies and their protection of personal information.

- To challenge assumptions of policy makers and other stakeholders – This research is interested in the perception of privacy and in particular, the email and Internet use policies of the organisations, combined with the culture within those organisations. The depth of concern for privacy issues discovered during the research allowed for the challenging of assumptions made within public policy and corporate policy regarding its protection.
identify areas of improvement of services needed – This research involved an
valuation of the internal culture and ICT use policies regarding computer use and
privacy protection. It was also interesting to discover individual perceptions of policies
such as the implementation of Closed Circuit Television in town centres, and the role of
the media as an information source.

The method can also be applied to uncover ‘alternative moral points of view’ (Denzin,
1989 p.11). Here an ethical viewpoint of the implementation and policies of the
organisation was studied. Denzin stressed that his method is for the interpretation of
lived experiences’. Here is perhaps the most critical part of the research. The point of
discovering the perceptions of the individuals involved, and how information
technology had effected their perceptions of privacy, was to discover how this had
effected their lives, and how they saw the world. This interpretation of the findings
clearly fits well with Denzin’s approach.

Interpretive interactionism maintains that ‘its emphasis on the uniqueness of each life
holds up the individual case as the measure of the effectiveness of all applied programs’
(Denzin, 1989 p.11). Having rejected positivist quantitative methodologies, this method
analysis fully considers the individual in their own context.

From an initial examination of Denzin’s approach, it was clear that there was a great
deal of scope for this methodology beyond his initial concepts. In this research,
though it is not within the closed field recommended by Denzin, there are correlations
with the goals and method of this form of enquiry that made it appropriate for this
search. The use of a hermeneutic approach which Denzin considered critical within
interpretive interactionism meant that these two approaches complemented each other methodologically. Further they ensured that the findings from this research enabled the discovery of perceptions of privacy by analysis of meaning, consideration of context and identification of key themes.

In this way hermeneutic interpretive interactionism provides this research with a rich source of information and tools to enable the perceptions of individuals within the organisations to be discovered. Further it provided an approach and framework that allowed the issues to be fully explored in such a way that focused on the experiences of the individuals, their interpretation and responses to the questions posed during the interviews.

The next section will continue to examine the methods used in this study in order to give a clear picture of the research project. An in-depth discussion of Denzin's technique of Interpretive Interactionism and the systematic methodology for its application is detailed below.

4. Case Study

In order to fully utilise the above techniques and approaches, it was necessary to give careful consideration to the methods used in the collection of data for analysis. Whilst several possible data collection methods were considered, the case study with its ability to discover rich and varied contextual as well as direct information was selected.

The case study method of social research was developed during the early 1900’s, the 'Chicago School' bringing this method to the fore. It has been defined as 'an in-depth,
ultifaceted investigation, using qualitative research methods, of a single social phenomenon. The study is conducted in great detail and often relies on the use of several data sources’ (Feagin, Orum and Sjoberg, 1991 p.2). Its conflict with positivist/scientific methods has however led to it being in and out of favour since its beginnings.

A case study is a method of research that focuses on a group, an individual or a phenomenon, in order to identify trends and issues or to answer specific research questions. The use of a case study approach enables the researcher to operate within clear parameters with pre-determined subjects for research that ‘strive towards a holistic understanding of cultural systems of action’ (Feagin, Orum and Sjoberg, 1991 p.4).

Case studies are useful when time and financial constraints prevent researchers from undertaking lengthy and costly longitudinal studies, and where, as in this research, an organisational as well as an individual focus is required.

It has been indicated by Feagin, Orum and Sjoberg (1991 p.6-7) that there are several factors, which defend the use of case study.

- It permits the grounding of observations and concepts about social action and social structures in natural settings studied at close hand.

- Information is gathered from a number of sources and over a period of time, thus permitting a more holistic study of complex social networks and of the complexities of social action and social meanings.
• It can furnish the dimensions of time and history to the study of social life, thereby enabling the investigator to examine continuity and change.

• It encourages and facilitates in practice, theoretical innovation and generalisation.

The case study is perfectly suited to studies using a hermeneutic approach due to its use of multiple methodologies for data collection and intuitive approach to analysis. This allows for a close and in depth scrutiny and interpretation of a specific group, phenomenon, organisation or individual to discover meaning. Case studies are used ‘to explain the causal links in real-life interventions that are too complex for the survey or experimental strategies’ (Yin, 1994 p.15, emphasis in original). It also ‘investigates a contemporary phenomenon within its real life context especially when the boundaries between phenomenon and context are not clearly visible’ (Yin, 1994 p.13). The main purpose of a case study is to explain, describe, illustrate, explore and evaluate phenomena.

Take (1994 p.4) identifies three types of case study. *Intrinsic* studies aim for a better understanding of issues within the case. *Instrumental* studies seek insight or the refinement of a theory and *collective* studies require that more than one study is undertaken in order to learn about phenomena or the general condition of the object of inquiry. When trying to ascertain the extent of individual perceptions of an issue such as privacy, it was necessary to undertake a collective study. This was to consider how the internal culture of an organisation might have affected the perceptions of its members and the influence of the participants on the organisation.
The multiple sources of data available whilst conducting a case study mean that there is a great scope for gathering diverse information and for providing rich data. This enabled the identification of feelings and perceptions during analysis, which may not have come to light if only one method of collection had been used. This is because a case study …can permit the researcher to examine not only the complex of life in which people are implicated but also the impact on beliefs and decisions of the complex web of social interaction’ (Feagin, Orum, and Sjoberg, 1991 p.9). This is in keeping withenzin’s approach to empirical study by considering the context in which the experiences of the individuals are placed.

Criticisms of the case study approach consider it to be lacking in academic rigor, or that gives little basis for scientific generalisation. The reason for this has been largely due to its interpretive nature. Criticisms include that ‘its dependence on a single case renders it incapable of providing a generalising conclusion’ (Tellis, 1997 p.3). This can however be overcome in part. Yin (1994) suggests that using four tests to establish the quality of the empirical research can overcome these criticisms.

1. Construct Validity - which identifies multiple sources of evidence, selects changes and demonstrates the measurements to be used. It also involves a review of the pilot study and previous reports. This will enable the researcher to ensure that they are asking the right questions.

2. Internal Validity - ensures that the methods are addressing the question.

3. External Validity - establishes the domain in which the results can be generalised to a theory and asks if the case study is representative.
4. Reliability - establishes whether the case can be repeated using the method and ensures that records are reliable and comprehensive.

Adapted from Yin, 1994 p.20)

Other concerns raised consider single case studies as unable to generalise or to formalise findings. However, in this study, not only was there a consideration of two cases with regard to the organisations involved, but within each organisational case there were eight to ten individuals who could all be considered case studies in their own right, thus refuting the problems of validity and single cases within case study.

Furthermore, it must be remembered that the use of the case study in this research is intended as a data collection tool and that analysis and approach are determined by the hermeneutics of Gadamer and Heidegger combined with the interpretive interactionism techniques of Denzin. It is therefore largely unimportant that the above tests are fully complied with. The analytical techniques used for this study are more than vigorous enough to allow for some flexibility in the use of case study as a form of data collection, which will be evidenced later.

.5. An In-Depth Analysis of the Methodologies Utilised

The purpose of this section is to clarify and detail the methods used for this study. As explained earlier, the approach of this research is a hermeneutic one, and has used case studies to collect the information and analysed using interpretive interactionism. Firstly, there is a detailed examination of the case study tools as utilized by this work, which explains the processes undertaken during the study. This is followed by an explanation
If the principles of interpretive interactionism to clarify the approach used during the analysis, and which is detailed in Chapter 5.

5.5.1. Case Study

When trying to ascertain the extent of individual perceptions of an issue such as privacy, it was necessary to undertake a collective study involving several case studies or comparable analysis. This made allowances for the possibility that the internal culture of an organisation may affect the perceptions of its members and thus enabling the discovery of perceptions beyond this influence. The multiple sources of data available for conducting this case study meant that there was great scope for gathering diverse information. This enabled the identification of feelings and perceptions, which may not have come to light if only one method of collection had been used. Therefore a case study…can permit the researcher to examine not only the complex of life in which people are implicated but also the impact on beliefs and decisions of the complex web of social interaction’ (Feagin, Orum, and Sjoberg, 1991 p.9).

The critical tool employed for this work was the interview. In this study, it was decided to interview the participants in a semi-structured way in order to enable sufficient flexibility and openness that would allow the participants to relax. It was discovered from the analysis that where participants were more relaxed, they were more likely to talk in greater detail and for longer periods of time. The more tense participants were much more likely to give brief answers to questions without much elaboration.

5.5.2. Interviews: An Overview
When conducting a case study, the use of interviews is highly valuable. They allow an
examination of perceptions and perspectives directly from the individual. They also
enable a rich and varied amount of information to be collected that can provide intuitive
insight into the phenomenon being studied. The reliability of the responses during
interview however, may create some problems for the researcher. The interviewee may
give answers to questions based on the 'appearance' of the interviewer, the responses
they 'think' may be required, or according to a 'public' face which bears little
semblance to their true feelings about an issue.

There is also a danger of the respondent being 'led' by the interviewer. This is
particularly a concern where the interviewer is also the researcher and who may have
reconceived ideas as to the responses expected. By being aware of this potential
problem, the researcher can take steps to minimise these effects by considering their
own responses to the participant's answers to questioning. By carefully formulating
subsequent questions, which do not present a particular viewpoint but allow expansion
within the scope of the phenomena being studied, new insight can be drawn. It has been
suggested that even the language used by interviewers may have a profound impact on
the data collected where 'individual interviewers would have consistent preferences for
the use of certain words, and therefore, would thus bias data collected' (Harper, Boyd

Once this is accepted and factored into the analysis, any bias brought into the work by
the interviewer can be considered and eliminated or at the very least, minimised.

However, the prejudice or hypothesis taken into the interview room by the researcher
in some way guides our observations, and helps us to select from the innumerable
objects of observation those which may be of interest’ (Popper, 1957 p.19). This enables the researcher to focus on discovering the information required by the study.

One-to-one interviews are useful in that they allow the subject to ‘warm’ to the issues and the interviewer too, thereby allowing insight to be discovered into the perceptions of the interviewee. Where the participant remains ‘cold’ to the researcher as in questionnaire or survey research, here the participants may consider that some questions are too sensitive in nature. In this case they may not wish to discuss these issues openly and personal thoughts may not be articulated. In other instances, surveys and questionnaires may not consider issues believed to be important by the participants. This may result in important perspectives and opinions being missed by the lack of scope in the process. The purpose of this research was to delve into perceptions and how the participants felt about the issues. This required the warming of the participant to their surroundings and the interviewer to enable the participant to become more relaxed and therefore open to discussing their feelings.

The use of semi or un-structured interviews was important to provide the scope and flexibility needed for this study. It enabled the responses of the subject to be considered in the formulation of interview questions and enabled the adjustment of those questions in response to previous answers. This allowed the interview to flow and to provide an in-depth response gained by informal discussion.

Interviews provide a rich source of data. Respondents can be asked for clarification in a way that they cannot with questionnaires and surveys. Interviews can also develop into depth discussions, particularly where a good rapport is developed between researcher
nd participant. If the researcher can direct the course of the interview to maintain a focus on the research questions, there is much scope for the discovery detail, which may become the focus of further study or the key to discovering previously hidden information.

### 5.3. Case Study Selection

In order to provide a public sector and private sector comparison, two organisations were studied. It was decided that a single case study would not provide sufficient insight. Denzin (1989) would argue that a single case is of significant magnitude to be valid for the study of an epiphany. However, the interest in the discovery of differences and/or similarities between individuals and organisations in privacy perception meant that the multiple cases within each organisation and the organisations themselves would be required to enable comparisons to be valuable. Another key element of interest was to discover if there was any difference in the approach to privacy and policies within public sector and private sector organisations themselves.

The criterion for selection of the organisations was that they should be large enough to have a significant number of employees that were engaged in computer use during their working day. Further, the public sector organisation is a medium sized local council, Inckley and Bosworth Borough Council, and in order to ensure that comparisons could be drawn, it was necessary to select a private sector organisation of similar size. Therefore, Alstec PLC was selected. Once the organisations were selected participants were drawn from several different departments so that privacy, and compliance with data protection legislation could be examined and individuals in a variety of different
jobs studied. Further details regarding the individual participants and the organisations involved are provided in Chapter 4.

The number of employees selected for this study was decided by consideration of the literature on qualitative methodologies (Cresswell, 1998; Denzin and Lincoln, 1998; Miles and Huberman, 1984). Ultimately it was decided that there would be a target of ten participants at each organisation. Although this was achieved within Alstec, circumstances beyond the control of the researcher led to only eight participants from BBC being interviewed. However, there was sufficient data collected from both organisations so that this did not adversely affect the study. A more detailed examination of the processes, analysis of the interviews and discussion of the contents of the documentation are given in Chapter 5.

Having set out the details of the interview approach above, the analysis process will now be discussed which clarifies the use of Denzin’s interpretive interactionism and details the steps to analysis that were undertaken through its use in this study.

The interpretive interactionism approach follows several key steps.

6.6. The Phases of the Research Process

6.6.1. Framing the Question

By using tools of interpretive interactionism it was possible to focus and formulate the research from the outset. Chapter 1 clarifies and sets out the research questions. The framing of the question involved setting the initial parameters for the research, and providing a starting point for the enquiry.
3.6.2. Deconstruction

Denzin saw deconstruction as ‘a critical analysis of how it has been presented, studied, and analysed in the existing research and theoretical literature’ (Denzin, 1989 p.51).

This part of the research process, involved a thorough review of the current and past literature in the field so that the research can be placed in context. This is also compliant with the hermeneutic circle, which places the researched, and researcher into the centre of the process. By analysing previous work in the field, the researcher was able to gain familiarity with the issues. The involvement in the culture of new technological implementation has also enabled this research to be conducted within its sociological context enabling immersion with the researcher and the researched. A thorough deconstruction and analysis of relevant literature and its cultural context is given in Chapter 2.

3.6.3. Capture

This involved the collection of narratives and the experiences from the subject, in their own words. For this reason interviewing was open ended, largely unstructured, adapted according to the individual, a conversation, and two-way.

In this case, the interview process enabled the individuals to give their explanations and experiences of privacy, how important it is to them and how technology has affected them. The interviews also revealed the life changing effects that information technologies have had, thus enabling the location of the epiphany necessary for Denzin’s methodology which is detailed below. By placing the concerns of privacy into the context of the organisations involved in the study, and also by discovering the wider
impact the issues of privacy are perceived to have had in society, the research has been
located in the modern world. The need for multiple cases was achieved by interviewing
number of individuals from each organisation, and from varying departments. The
interview data was the main source of information captured for this research.

1.6.4. Bracketing (Reduction)

In the first instance it was necessary to read the narrative and place oneself into the
context of the story, in the place of the teller, to achieve an understanding of the
problems and to ascribe meaning to what is said. The process refers to the use of key
words and terms, and the use of metaphor and simile to arrive at themes, which assist
understanding.

Bracketing referred to originally by Husserl (1931) involves taking the phenomena out
of the worldview, dissecting it and uncovering its essential structures. The subject is
then confronted on its own terms. In this way, the transcripts of the original interviews
were closely analysed and themes identified across the whole of the research. Each
theme was then further studied to discover further elements. This provided the first
critical step in the analysis and was important to enable the identification of the
epiphany which is a key element in interpretive interactionism.

.6.5. Epiphany – Transformational Experiences.

Locating the epiphany in interpretive interactionism is one of the starting points for
analysis. This is where the experiences that have had a transforming effect on the
individual concerned are identified. In the case of this research it was represented by
The kinds of impact computers have had on the daily lives of the interviewees. It is clear that computing and information technology have had an immense impact on all our lives. The process has been relatively rapid and can be seen as life changing, and even if it has not been a single event, it can be considered to be a major transformational experience for society and the individuals within it.

Although in the cases cited by Denzin, these 'epiphanies' are often violent or disturbing, the life transformation aspect of the introduction of computers has had as great an impact on individual lives, which in some cases may have been traumatic. The phenomenon of technophobia, although not explored in this thesis can be seen as traumatic and life changing to an extent not unlike those suffered at the hands of a violent person. This is not to denigrate the appalling experiences of victims of such acts, but identifies that a traumatic or life changing experience does not have to include error or violence in the physical sense, but may also include change or fear of change that may have a profound effect on the individual.

The effect of the epiphany may range in severity from a growth, acceptance and identification of the benefits of change, to a rejection of technology and a refusal to engage in such a change for fear of failure, or a lack of understanding. To return to Denzin's argument, the transformational experience therefore, may produce negative notional responses to those situations, or a positive embracing of change. Whichever way this is viewed by the participants in the study, an epiphany may be good or bad, but is certainly a life changing experience.

6.6. Construction
y listing the bracketed elements of the phenomenon and placing them in order as they occurred originally, it was possible to see how each process during the interview affected the other. In this way, there becomes a clear path, which indicates how each theme adheres to the other and the order in which they occurred. This process clarified the text and formalised the narrative to:

- Locate the narrative within personal experience.
- Interpret the meanings.
- Obtain the subjects interpretations.
- Locate the epiphany
- Inspect what the findings reveal.
- Offer a tentative statement or definition.

6.7. Contextualization

This stage required that the themes were located within the personal experience of the interviewee in order that interpretation of meanings can be undertaken. It is at this stage that the full influence of the individual comes to bear. Each interview subject will have brought his or her own pre-judged ideas, experiences, influences and ideas to the project.

Other influences; age, experience, position within the organisation will also have an impact and need to be considered where meanings are being interpreted. It is also important at this stage that awareness of the researcher and their personal prejudice...
combined with the inability of the researcher to take a distanced view from the phenomenon should be considered in the context of the research results. This will ultimately enable the researcher to locate the subject by placing the individual in their social context.

Therefore, contextualization attempts to interpret structures and themes disclosed in racketing and construction and place it in the social world and personal biographies of those involved to:

- Obtain and present personal experience that details the essential features of the phenomenon.
- Present contrasts.
- Indicate how lived experiences alter and shape the features.
- Compare and synthesize the main themes.

The intent of contextualisation is to show how lived experience alters and shapes the phenomenon being studied' (Denzin, 1989 p.68).

Denzin’s descriptive technique, ‘thick description’ requires that all meaning is seen as symbolic, operates at all levels and therefore gives a high degree of detail. It is expected that during the thick description of the research, interpretation, i.e. deciphering intentions and actions will lead to the clarification of meaning and enable understanding. There are two key elements to be discovered by this process, firstly the
motional (that which interpretive interactionism tries to unveil) and secondly cognitive meaning but not emotion) interpretation.

Nick description and interpretation are critical elements within interpretive interactionism. One should use this approach ‘if one’s goal is to understand and interpret the world as it is lived, experienced and given meaning’ (Denzin, 1989 p.34). The above tools represent a framework that enables the completion of this study in such a way that the initial research questions can be answered.

6.6.8. The Interpretive Process

What is really intended through the use of Denzin’s interpretive interactionism is that the research should be located within individual personal experiences, so that the research is as real and close to true experiences as possible. It was not intended to objectify or distance the research from the subject as in positivist research. Rather, it was intended to discover individual perceptions of the impact of ICTs on privacy, and to interpret its meaning in the context of the organisations in which the subjects are based, and their societal view. This has enabled the research to re-create lived experiences that define the phenomenon under inspection.

6.6.9. Steps to Interpretation

Here are several steps to interpretation that were identified by Denzin. Each provides a structure and series of check points to ensure that the study is rigorous and has validity once completed.

- Securing the interactional text (collation and ordering).
- Displaying the text as a unit (consideration of the whole picture).

- Subdividing the text into key experiential units (deconstruction of the data).

- Linguistic and interpretive analysis of each unit (further deconstruction and identification of themes).

- Serial unfolding and interpretation of the meanings of the text to the participants (placing the data into cultural and personal context).

- Development of working interpretations of the text (consideration of the key findings for further analysis).

- Checking these hypotheses against the subsequent portions of the text (where no previous hypothesis has been formulated, enables theory development).

- Grasping the text as a totality (understanding the whole picture).

- Displaying the multiple interpretations that occur within the text (the differences and similarities in responses and cultural effects).

Adapted from Denzin, 1989 p.46)

**6.10. Situating Interpretation**

The final step in interpretation was to situate the discoveries within their own context. Firstly the timing of the data collection needed to be acknowledged, to discover in what specific atmosphere the interviews took place. In the case of Alstec PLC, the study was
undertaken just after a management buy-out when the major restructuring of the workforce had been completed and an overhaul of its management culture had been implemented. Hinckley and Bosworth Borough Council was in the process of intense data protection training in anticipation of the full force of the legislation becoming imminent.

In order to place each case into context, it was then necessary to look at the history of the organisations in a broader sense. This was to discover the culture within them, and how this had changed with the introduction of ICTs. Next, the study was placed in context from the perspectives of those directly involved. This required consideration of their position within the organisation, age and their length of service. These results were then analysed from individual perspectives concerning their interactional situations. Finally, the differences between public sector and private sector culture, newcomers and long term employee perspectives, and how they interpret their experiences and perceptions was examined.

6.1.1 Evaluation

Once the previous stages of analysis had been undertaken, there were several questions that needed to be asked to ensure that the study has worth, validity and completeness:

- Do they illuminate the phenomena?
- Are they based on thickly contextualized materials?
- Are they historically and relationally grounded?
- Do they follow a process and are interactive?
• Do they engulf what is known about the phenomena?

• Do they incorporate prior understandings of the phenomena?

• Do they cohere and produce understanding?

Once these questions were answered in the affirmative, it could be concluded that the results of the study were completed as far as the hermeneutic circle may be, and that to be able to discover any further information would require further data collection and study. It is at this final stage that the research project was considered to be completed.

By following the above techniques from a hermeneutic approach it has been able to discover the meaning of the interview data. This means that the information gathered contained the answers to the original research questions, and the interpretation techniques utilized has further allowed the research to discover new insights into the phenomenon, and to discover meaning in the data collected.

3.7. The Research Approach

This section sets out the research project in detail, providing a comprehensive view of the steps taken to undertake this research, a model of the project and a framework for the analysis of the information gathered during the interviews.

The model in figure 3.1 indicates the stages of the research project from initial contact with the organisation, the interview phases and analysis leading to the conclusions and results inferred from the research. It details the interactions between each part of the
research process to provide a better understanding of the approaches of interpretive interactionism, hermeneutic enquiry and intuitive methods as utilised in this research.

The continuous interactions between each part of the study enabled it to be placed within context and to consider each influencing variable as it is uncovered.
As can be seen from figure 3.1, the research was conducted in nine steps.

**Step 1** – The deconstruction stage where the literature was reviewed and analysed in order to place the research into context and to consider previous work in the field. This stage involved the formulation of the research questions from the perspective of the approach taken.

**Step 2** – The initial contact, where the selection of participants was undertaken. This was completed either by the organisation and researcher together as in the case of Alstec or by the organisation itself as in H&BBC. This step also included the sending out of invitations to participate, and the re-selection of an interviewee in the case of a refusal. At this stage the interview dates were arranged and a location selected.

**Step 3** – The next step in the research process was to undertake the interviews. This was the capture of the data for analysis as indicated within the tools of interpretive interactionism. Each interviewee was asked to sign a consent form to indicate willingness to participate, and permission was obtained to tape record the interview. As the interviews occurred in two parts, and the analysis of the first interviews was underway during the time that interview two was being conducted, there was a merge of step three and step four.

**Step 4** – During this stage, transcription of interviews and analysis of the data were undertaken. This involved the process of bracketing the data into themes. As mentioned previously, the cross over effect of the two phases of interviews meant that
Phase three and phase four were conducted simultaneously. Once the second interviews had been completed and transcriptions made, analysis of the data in earnest was undertaken.

**Step 5** – This phase of the analysis was also concerned with the development of themes and bracketing the data undertaken to compare and contrast the first and second interviews. This was to discover the changes in privacy perception prior to and post first interview. This analysis was undertaken giving due regard to the Hawthorn effect, which considers that being a participant in a study may affect the results.

**Step 6** – Once the analysis of each organisation was undertaken, the results were then constructed by identifying public/private/individual perspectives. This resulted in three distinct areas of analysis.

**Step 7** – The results and conclusions from steps four and five were correlated for each organisation, resulting in further construction of the results.

**Step 8** – The results and conclusions from steps six and seven were merged and contextualised to provide insight into individual perceptions of privacy. This allowed for the input and influence of the organisations and other external factors such as the media, whilst maintaining consistency in maintaining a focus on the individual.

**Step 9** – The contextualised results of the study were then evaluated to discern the overall conclusions and discoveries of the research.
The nine steps above were ways of formalising the intuitive process, which was ongoing and interpretive throughout the study. Therefore, although the steps have been identified, this is not to say that each one was strictly adhered to in sequence. As has been explained previously there was a considerable amount of cross analysis between each step as themes emerged and the analysis progressed. Below indicates in more detail the framework that was kept in mind throughout the analysis.

6.8. Framework for Analysis

In order to maintain focus on the point of the study, and to discover the answers to the research questions, it was necessary to formulate this framework. Without clear guidelines, it would be far too easy for the researcher to drift from the original aims of the research and therefore be unable to answer the questions posed at the outset of the study. However, it should also be remembered that the intuitive and hermeneutic approach to this research requires that ultimately, it is the discovery of the perceptions of those individuals involved that is important, and not those of the researcher, requiring a flexible approach to the analysis as well as the data collection.

As this thesis has concentrated on discovering individual perceptions of privacy, five initial areas of enquiry were considered during the analysis with a further three influences also considered to enable perceptions to be discovered. These areas of enquiry and influence, whilst not exhaustive, were selected as the critical indicators for perception discovery. As individuals may have different reactions to the same experiences, the consideration of several areas of enquiry within the project enabled
These factors to be utilised during contextualisation of the study. The five areas of
enquiry and three influences are detailed below.

Other areas of enquiry that may have been investigated were considered to be less
important and any increase in the number of areas of enquiry for analysis would have
entailed a mere skimming the surface. Keeping the number of areas of enquiry to five
and influences to three has enabled a more in depth and focused analysis to be
undertaken.

3.8.1. Importance

When perceptions need to be analysed, the importance of an issue, as indicated by the
respondent, can be gauged by the strength of a response to a question. For example,
where someone is asked about the use of personal information for commercial ends, the
type of response gives an indication of the perceptions of those individuals regarding
that issue. The importance of the issues discussed enables the interviewer to gain
insight into the perceptions of the respondent.

It was necessary to initially discover the importance of privacy to the interviewees.

The degree of importance of privacy to each individual was analysed by looking at the
trength of wording given by the participants to questioning. This involved looking at
the responses to questions regarding issues such as CCTV, Junk Mail, Personal
Information, and the Internet. In this way the strength of the responses to such
questions provided a clear indication of the importance of privacy felt by the
individuals.
Analysis indicated that in some cases, importance became more strongly felt as the interview progressed and in particular between interview one and two. It was interesting to note if the importance of the issues was raised due to an increased awareness as the interview progressed and issues were discussed.

It was also considered whether the reason for this was due to unconscious thought, influenced by an awareness of the issues from previous experience, media etc, which may not have been considered in any depth by the interviewee before. Earlier responses may therefore be due to conditioned or ‘gut’ reactions rather than a conscious consideration of the issues discussed. It may be that the interviewees initially tried to give answers that they thought the organisation would approve of, or what they thought the interviewer expected. It may also be that they felt uncomfortable at first and as they began to relax, they were able to think more clearly about the issues raised. By examining the interviews in sequence as well as thematically, it was possible to discover how perceptions changed during the interview and to what extent.

8.2. Awareness

This could initially be considered as similar to importance. However, awareness differs in several key respects:

The degree of importance felt by an individual may be quite different to their awareness of what is actually happening.

It was clear from the analysis, that the degree of importance felt, was not only dependent on the level of awareness, in that one may feel less importance towards
issues about which one is less aware, but that we may also be less inclined to find out and become aware of the facts behind the issues that we consider unimportant.

A lack of awareness of issues may mean that the degree of importance felt may be based on insufficient knowledge of those issues, which may lead to a greater or lesser perception of importance. Therefore, awareness of the issues had a major impact on the perceptions of the individual and the importance given to the issues discussed.

Awareness of the issues may be high and yet considered of low priority or concern and therefore largely unimportant. An example being Participant J (see below) whose marketing background equipped him with considerable awareness of the privacy implications from a commercial perspective, but who considers use of his personal details to be important for the benefits of marketing and of little concern with regards to the loss of privacy this may entail.

The discovery of how aware participants were to privacy issues involved a cross-referencing to the issue of importance, to see how each influences each. Does greater awareness affect the importance placed on privacy? This was particularly interesting with regard to the possible change of emphasis during the course of the interviews. Whilst it is clear that the entire process was an awareness raising experience, it was important to discover the degree of awareness at the outset. This was then followed by analysis of how far the process of research had raised the awareness and the impact on individual perception of importance.

8.3. Is Privacy Seen as a Right?
This fundamental question was asked directly during the second interview. Although his question was not directly a general area of enquiry, it was purposely designed to elicit a reactive response, which was then followed up with further questioning. This was because there would be some impact of being involved in the study, and the presence of the researcher. Therefore, the nature and type of questioning would have raised the participant’s awareness about the issues.

The question was asked to gain some indication of whether ‘ordinary’ people believe privacy is a right, and to help to decipher unconscious and conscious thought in their responses to the question. By asking such a direct and yet difficult to answer question, enabled the research to gain insight into perceptions about the key issue of privacy, that less direct questioning was unable to do alone. This was because, the use of such a direct question provoked a ‘gut’ reaction in the first instance, which gave an indication of perception not necessarily based on participants trying to answer the questions according to the researcher’s expectations.

His controversial issue was discussed directly with the interviewees. Initial analysis revealed a problem with perceptions of privacy as a right. All interviewees considered privacy to be a right regardless of age, position within organisation or length of service and yet when asked to explain their answer, participants were generally unsure how to reply. This analysis served to highlight the similarities of the caveats discovered during the responses to further questioning on this issue. Therefore it was possible to discover when it was considered appropriate that certain anti-social behaviour would result in a subsequent invasion of privacy by relevant authorities such as the police.
.8.4. Effects of ICT

his area of enquiry was one of the most important factors to consider. Therefore, it was important to discover how individuals felt regarding the impact computers and information technologies have had on the way they work, and their personal lives. ICT user policies within the organisation were analysed to discover the perceptions of those issues from an organisational perspective. Further, the extent to which individuals within the organisation complied with these policies was important to consider individual and organisational perspectives. It was important to discover the extent to which the use of ICTs had become an intrinsic part of individual's working and personal life, and how far the gathering of personal data had become an accepted part of modern living and participation in society.

ICTs have undoubtedly had a direct influence on the ability to both ensure privacy and undermine it. Analysis of this issue focused on aspects such as surveillance, computerisation, data-bases, and the Internet. Questions included those, which asked for an analysis of their perceptions of expectations of privacy in the past and in the present day. It was also analysed what the interviewees' perceptions were of the impact of computing on the privacy of the individual in the ensuing years.

It was interesting to note how the individuals' age, position within the organisation and length of service or length of service had affected their perceptions of ICTs and its effect on privacy.

.8.5. The Role of the Organisation
This was important in establishing perceptions for several reasons; the level of training and internal culture of the organisation may have had a direct impact on the perceptions of the individuals within the organisation and vice-versa. Furthermore, the type of the organisation in this case, whether it was public or private sector, may have had an impact on the perceptions of individuals. By looking at the role of the organisation in shaping awareness, and importance of privacy, plus the strength of the organisation's privacy culture it was expected to uncover some of the influences on perception. The effects of individual influence on organisational culture and policies were also considered. The policies of the organisation with regard to the use of ICTs and the degree of computer use/email use within the organisation were also factors which would have an impact upon individuals within the workplace. It was therefore interesting to note similarities and differences between members of each organisation and their perceptions of privacy within their personal lives.

Concurrently to the above areas of enquiry, the analysis undertook to consider three key influences on individual and organisational perspectives.

.8.6. Age

The growth of the use of computers to its application in almost every area of life has been rapid. Therefore, there must be some consideration of the impact of this growth on different age groups. Initial researcher expectations were that older people may be less comfortable with computer use and more concerned about privacy issues than younger people. However, as is shown in the findings below, this was not the case in this search, showing little significant age difference in the analysis. It should be noted that
his study was not intended to consider age as a key factor for the analysis, but rather that age was to be seen as an influencing factor. Had the research been more age focused, then different findings may have been uncovered.

### 8.8.7. Position in Organisation

This was seen as a key influence on the perceptions of the interviewees for several reasons. Those in higher positions may be more aware of the importance of computer use from an organisational perspective, perhaps from being involved in policy formulation or key decision making. They may be more concerned with the impact that ICTs have had on employee efficiency.

The interviewee’s position within the organisation may also influence their perceptions of personal privacy which may further link to the above investigations of importance, awareness and so on. That was particularly of interest where personal perspectives were analysed outside of the work context.

Other factors which were aspects of this influence were the levels of training and experience that the interviewee had, and the length of service within the organisation. In some cases, older and more senior employees had seen the implementation of computers from the start and may have been able to see with some clarity and experience the impact of ICTs on their work, organisation and personal lives. This therefore was likely to have considerable influence on individual perceptions and which the analysis uncovers.

### 8.8. Length of Service
This factor was seen as influential in particular with regard to the organisation and the effects on individuals. Therefore, it was expected that those with longer service records would have a stronger leaning towards organisational perspective on privacy than those with shorter employment history. There was an expectation that those with longer service would also be able to provide greater insight into the internal culture of each organisation and to identify changes and differences they had noticed since the introduction of ICT technologies.

By analysing the influence of the position within the organisation, the age of employees and length of service, perceptions were discovered and influences acknowledged. Other personal influences were not directly investigated during the course of the interviews although in some cases, some information was volunteered, such as experience of inappropriate release of data, and problems with marketing telephone calls. Clearly, personal experience of problems with the use of ICTs and privacy protection is likely to have made some interviewees more aware of the issues.

All of the above factors therefore enabled the research to be conducted hermeneutically by placing the information into context, and to follow interpretive interactionism for the analysis by considering the ‘lived experiences’ of the participants.

**9. Conclusion**

From the above analysis and discussion, the approach, techniques and tools for this search have been detailed. It has been made clear how the use of a hermeneutic approach was appropriate for this research and that the tools outlined by Denzin provided a framework for the project. A powerful tool based on Denzin’s methodology
as been developed providing a unique method for the study of privacy perception. The use of case study for data collection has been described and how the utilisation of the above has enabled the research findings to be discovered. The following chapters put these perspectives into practice and provide the reader with hard data and analysis from the field work.
Chapter 4: THE CASE STUDIES: DESCRIPTION OF ORGANISATIONS AND PARTICIPANT PROFILES.

There are several reasons for choosing these two organisations over the vast number of potential subjects for case study.

The public/private contrast was interesting to examine the culture of two organisations.

The local base of both organisations meant that the research could be undertaken with minimum outlay for travelling expenses and time.

The organisations were selected for this study because they reflected public and private perspectives on the issues and provided valuable insight into privacy perceptions from both approaches. By choosing interview subjects from a diverse range of positions and ages within the organisation, it was felt that some generalisation would be achievable as perceptions within the organisations studied. This would not be reliant on any previous knowledge of privacy policies or personal privacy protection before the interview. It was important to discover how individuals perceive privacy within the organisation and from the organisations culture rather than from a knowledgeable and therefore possibly slanted perspective. This may have been the case if just one section of the organisation had been identified for this research.

The use of a hermeneutic approach to the research provides sufficient scope to enable themes to emerge, which may not occur during more quantitative research. There were some similarities between the two organisations selected. Both were concerned with ensuring that the legal aspects of their business are adhered to. From Alstec’s
erspective this meant compliance with for example, the Official Secrets Act, due to the sensitive nature of some of the projects undertaken. From H&BBC’s perspective this meant ensuring that, for example, the Freedom of Information Act 2001 was enforced and any information requested was made available. What was expected to be discovered from this research was whether there were any significant differences in approaches to privacy and privacy protection between the organisations and whether the employees had different or similar attitudes to the issue of privacy. What was also considered was whether individuals had different attitudes to privacy, and whether they were due to the internal culture of the organisation or if it was based on a more personal and individual perspective.

1.1. Case 1 - Alstec PLC

Originally formed in 1891, Alstec Plc, better known locally as GEC had been a strong presence in the local community. Although there had been name changes and restructuring over the years, Alstec continued to be one of the key engineering employers in the area. Alstec Plc was a medium sized organisation, which employed approximately five hundred staff. Most employees were located at its head office in Leicestershire, with up to one hundred staff located, on site, at various locations both in the UK and worldwide including offices in France and Spain. Alstec’s business concentrated on medium to heavy engineering for nuclear and thermal power plants, airport baggage systems and defence equipment. A recent restructure and re-naming of the company (from Alstom to Alstec) combined with a management buy-out in 2000 meant that the organisation was undergoing considerable change. The company website located at www.alstec.co.uk was a professionally designed and informative site which
erved to indicate the way the company had embraced new computing technologies in recent years. Alstec provided computer and Internet access to all office based staff, with skilled/manual workers offered this service on request. There were about six hundred and fifty registered users and on average about half of these logged into the e-mail system and the databases daily. This was an increase in a little over a year of one hundred since Lotus Notes and new servers had been installed.

There was a community spirit evident within the organisation, which may have had much to do with its strong local roots. This was because many of their staff was drawn from the local population. However, there was concern amongst some employees that certain changes and re-structuring was undermining this culture with the loss of the company social club, and some change in emphasis towards a greater drive for profit. There was some criticism of their approach to redundancies; investment in people type of thing isn’t really their forte (Participant F).

However, the organisational culture overall seems to have changed in a more positive way according to many employees. Since the management buy-out in 2000, the management team had been working to update and change the culture within the organisation. Employees who have seen the changes indicated that prior to the buy out, the culture was more restrictive and less trusting of the employees, with clocking in times and a considerable lack of flexibility. It was clear that attempts were being made to change this, with the introduction of time sheets, the abolition of clocking in, and the encouragement of a more trusting culture.
flexible approach to Internet access allowed employees to use this facility for personal reasons provided it was outside working hours. There were few promotion prospects within the company, with progression only likely if someone was to leave. Management was aware that the present induction process was poor, with little training prior to entering the job including a learn-as-you-go culture. The management indicated that they were working towards improving this, although practical measures were not outlined. There was little or no sponsorship for employees wishing to pursue education or to gain further qualifications even where this would benefit the company. Employees were largely expected to undertake further training in their own time and at their own expense. However, the organisation was willing to support research endeavours, as evidenced by their willingness to accommodate this research, which included the use of company equipment and access to personnel.

The computer systems were in the process of upgrade with the old mainframe computer being phased out and PC's being introduced company wide. There was some evidence of downsizing within the company, which may have been due to restructuring since the management buy-out. There was little indication of a fall off in trade or economic problems within the organisation.

Access to the organisation was secured by an initial telephone call followed up by a letter further outlining the research proposal and what was required of the company. The overall approach towards the research project was one of helpfulness and interest. It appeared from the outset that the company welcomed the opportunity to support the search and to facilitate the needs of the project. It was indicated that it was company
policy to actively support research and development in fields of study even if it was not directly related to the immediate needs of the company.

1.1.1. Alstec Plc Organisational ICT Policies

Alstec Plc had adopted a liberal approach to the use of ICTs within the organisation. In order to facilitate this, all members of staff apart from those on the shop floor who did not use a computer, had Internet access and email facilities on their desk. The ICT use policies had therefore been designed to reflect this attitude. There were two policies for consideration here.

1.1.2. Internet Usage Policy

This was created for the use of staff on January 3rd, 2001 and was designed by the IT manager in collaboration with other senior staff and taking input from senior IT support personnel.

The policy began with an introduction giving an overview of the philosophy regarding the use of the facilities. It clearly stated that it was ‘a freely available resource to all employees and contract/agency staff’ and that it was provided primarily for business related tasks. The overview stated that users should conduct themselves honestly and to consider ‘copyright, software licensing rules, property rights, privacy and confidentiality, and company information security issues’. Users were reminded of the problems of server congestion being caused by unnecessary use and the problems of unlawful or insensitive use. The policy then continued to detail the provisions of Internet use.
4.1.2.1. Section A - General

The first point clearly stated that there was monitoring software in place and that 'no user should have any expectation of privacy in respect of their Internet access activities'. This statement is of particular interest considering the lack of awareness of the monitoring capabilities of the organisation by some employees (see Chapter 5). This was a cause for some concern as it may indicate that those staff had not familiarized themselves with the policy and could therefore find themselves in a compromised position at a later date.

The organisation clearly stated in point two that they would inspect files to ensure compliance with the policy and point three regarding viewing, archiving, editing or distribution of sexual content was clear and unambiguous. However, as indicated by participant H the organisation was aware of the problem of pop-up advertising and so would operate the view that there was a distinction between intentional and unintentional viewing of such material. The policy further stated that although they were attempting to block such sites, they were aware of their rapidly changing nature. Employees were therefore advised that accidental connection to such sites should be terminated immediately.

The next main point discussed in the policy document was with regard to the laws and regulations of the United Kingdom. This maintained that employees must make every effort to ensure compliance with both UK and international law, and that the organisation would co-operate with 'any legitimate law-enforcement activity' (page 2, section A paragraph 5). However the Data Protection Act 1998 was not specifically detailed in any part of the use policy, nor was a link or reference to further information...
Although there was emphasis on the protection of information, it was not related directly to the Act and could be revised to include this.

The organisation then stated that all downloaded software would become the property of the organisation to be used consistent with licenses or copyrights and that pirated or illegal software was not permitted on the network. This then went further to discuss the use of the company’s facilities to knowingly use, propagate or download virus or virus laden software or to commit any act which may disable, overload or circumvent the security of any computer system.

The policy then outlined the responsibilities of users in the form of correct identification, and company affiliation where necessary and that only those with prior authorization where permitted to communicate the views of the company to the press or any other form of media. Alstec also maintained that ‘the company retains the copyright of any material distributed by a user in the course of their duties’ (page 2, section A, paragraph 12). This clearly indicated that the company by taking on this role considered that employee’s opinions regarding the company should only be disseminated according to the guidelines above. By taking ownership of distributed material, the organisation therefore took responsibility for the protection of company reputation.

The policy then went on to expand upon this by detailing the need for employees to ensure that company secrets, policies and procedures were not released and that anyone seeking those rules would be subject to disciplinary proceedings. Further points guarding such potential abuses of the company name, and facilities reiterated this point.
by going into further detail of what was unacceptable behaviour such as sexual harassment and misappropriation of intellectual property.

In the policy it clearly stated the conditions under which employees could use the facilities for personal web browsing 'users may use the Internet facility for personal web-browsing purposes, but should restrict their personal use to meal breaks and other out-of-hours times' (page 2, section A, paragraph 15). This contained a reiteration of he need to comply with the above points.

The final general points made by the policy included the need to take care to comply with copyright and similar laws, and that games and other software should not be downloaded or distributed. It also stated that company software should not be distributed without permission and that streaming services such as radio or video should not be used unless specifically for business purposes and with permission. The above stipulations were to avoid overloading the available bandwidth.

1.2.2. Section B – Technical

This section contained three points of concern for users with regards to their personal workstation. First was the requirement that only authorized users should be allowed access to the network and that passwords should be used and changed periodically to ensure security.

The next two points were with regard to the virus protection software. Firstly it advised employees that all downloaded files should be scanned prior to opening them and virus
infected files should be deleted without opening. Finally, users were advised that the virus protection facilities should not be disabled.

1.2.3. Section C - Security

This section indicated that protection measures had been installed to limit the use of the system and to prevent inappropriate use. It also stated that this would be periodically revised. Moreover, the policy stated that ‘only those Internet services and functions which serve business purposes will be enabled for general use’ (p3. section C, paragraph 2). This section further reiterated that the system was monitored, but was fairly vague in its wording.

1.2.4. Acknowledgement

The policies then stated that all users were expected to be fully aware of the policy and that by using the facilities accepted this obligation. It further stated that revisions to the policy may occur periodically, whereby all users would be advised by email.

When considering the policy above, it was clear that an attempt had been made by the management team to provide the use of facilities for working purposes, which were neither restrictive nor too indulgent. The staff interviewed agreed that the policy was fair and reasonable. It largely followed similar guidelines of Internet usage that some were familiar with from working in previous other organisations. Overall, the policy was clear and concise with little complex terminology. However, to improve the effectiveness of the policy it would be helpful to include a direct reference to the obligations of the Data Protection Act 1998 and a more explicit explanation of the security measure in place.
1.2.5. E-mail Usage Policy

The email usage policy was produced and distributed on the same day and by the same team as the Internet usage policy. This followed the same format and tone but with changes in terminology to reflect the use of email. Additional email restrictions included that users should not participate in chain mail and that virus-infected mail should be forwarded to the notes administrator prior to deletion.

Again the policy was considered to be fair and reasonable by all staff.

1.2.6. Summary

There was evidence that the management team in writing these policies had attempted to produce a document that would allow free use of the system whilst protecting the interests and reputation of the organisation. It was also designed to ensure that personal use was appropriate and did not overuse the system.

Here had been some abuse of the system detected but the management had decided that rather than taking a draconian attitude to this, that they would publicise its discovery by mail memo. In this way it was expected that the memo would reinforce the standards required in the policy and indicate that monitoring was in operation. Downloading of music and other files was prohibited by the policy, as was accessing of ‘inappropriate’ web sites. In this instance, inappropriate web sites were considered to be pornography or anything, which could be seen as insulting or dangerous to the company’s corporate image.
The management was aware of the problems associated with pop-up advertising. They were keen to consider overall web behaviour, length of time on sites and frequency of visits to those sites rather than enforcing disciplinary procedures for incidents where inappropriate sites had been accessed. Email was restricted in its content to include no defamatory statements or inappropriate language and included a standard disclaimer statement at the end of each email to cover liability.

The policies allowed staff to use the Internet for personal use outside of working hours, i.e. during lunch break and in the evenings. This flexible approach was seen as realistic by management in that they appreciated the need to use this service during office hours in the same way as the ability to make a phone call in an emergency was seen.

Overall, the policy appeared to be fair and reasonable, and the staff generally agreed with that analysis. One key point however, was that those staff who did not have desk access to the system perceived the use of the Internet to be too great, thinking that staff were accessing sites in working time. This showed a ‘them’ and us’ attitude within the organisation that the management were possibly not aware of. It was clear that all staff should have been made aware of the personal use part of the policy to avoid manual staff believing that the office workers were wiling away their time on excessive personal use of the Internet.

Overall, employees considered the policies to be fair and reasonable. There had been very little discovered abuse of the system and management were happy to allow open access to continue.
4.2. Case 2 - Hinckley and Bosworth Borough Council

Hinckley and Bosworth Borough Council (H&BBC) was a local government organisation, which covered a largely rural area with a population of 97,699 (1998 estimate). The council was perhaps lagging behind in its take up and use of computing technology, with many old computers and systems still in use. Whilst this equipment was being upgraded, the timescale appeared to be in years rather than months, largely due to budgetary concerns. It was only within the previous year that the council had begun to take seriously the concept and use of new computing technologies. One interviewee commented that they considered the council to be at least five years behind the times with its implementation of computing technologies. Since beginning the research, attempts had been made to update the available resources, including a more informative web page available at www.hinckley-bosworth.gov.uk, which was a significant improvement from the original single page that had been its online presence prior to this update.

Only staff members deemed to need email and the Internet had been permitted access, with firm controls on availability of that access. There was a very strong public service culture running throughout the council and great concern to prevent the misuse of council funds hence the strict controls on Internet and email use. However, the caution may have also been due to the relatively recent take up of the technology which had led to particular caution as to its use. Further, the public sector nature of the organisation meant that management considered that personal use of public funded facilities would be inappropriate.
There was much scope for personal development and training within the council providing there was money in the budget for that particular year. During the time that the research was being conducted, all staff underwent data protection training. The data protection training had led the staff to become very aware of the protection of personal information. In some cases compliance with the Act had been seen to be a little overzealous. This may begin to relax somewhat once employees became more familiar with it. The public policy elements of the research and the local nature of the council meant that it was ideally suited to discover the differences and similarities between public and private organisational attitudes towards privacy and policies.

1.2.1. Hinckley and Bosworth Borough Council Organisational ICT Policies

In stark contrast to Alstec, the H&BBC ICT use policy was much less flexible. It did not allow for any form of personal use. There were several reasons for this approach:

- A complete ban required less monitoring.
- Concern over private use of publicly funded equipment.
- Concern over the relative ‘newness’ of the technology leading to a cautious response.

The tone of the use policy was one of caution. From the outset, employees were advised that if there was an alternative to using the Internet, employees should choose that route. As stated earlier, some interviewees considered that H&BBC was some years behind others in the take up of new technology. This may indicate the reason for
strictness of the use policy in contrast with the more relaxed attitude of Alstec which embraced ICTs for some time. The policy produced by H&BBC was a single document encompassing both the use of the Internet and email.

2.2. Acceptable Usage Policy for E-Mail and the Internet

The document discussed below was a draft produced during August 2001 by the ICT services division of the council. Although subject to change, it was considered to be likely that little would alter in its final application. The policy first set out to indicate an awareness of the increasing importance of Internet and Web-based technologies whilst raising concerns about risks in its use.

2.2.1. Section A – General

The first point made was to strongly emphasise that the provision of the services was for business use only and that personal use was not permitted. This was written in bold to provide emphasis. The policy then went on to explain how only authorised users may have access and that approval must be applied for and given by management before use could begin. The approval procedure included a requirement to sign a declaration stating that the policy had been seen and would be adhered to. Further reiteration of the need to comply with the ICT use policies of both the Council and the Internet Service Provider were then detailed.

The policy explained the difficulties that may arise with the service and the expectation at employees would comply with requests to suspend use if required.
There was a large section (paragraph 7), which detailed the problems of the Internet being 'an inherently unregulated technology' and stressing that it was therefore insecure. This section also stressed the need to comply with the Data Protection Act 1998 for the processing of personal data, and that any documents requiring high levels of confidentiality should be delivered by alternative methods. Monitoring of the system was mentioned in the policy (paragraph 8 and 9) and it clearly stated that the management would access personal files for inappropriate content when it considered it to be necessary. The distribution of inappropriate material was also forbidden in the policy.

The next section clarified the risks of infringing copyright and licencing laws.

Paragraph 12 stated that pornographic and similar material should not be accessed, but allowed for accidental contact and advised users to report this to the ICT department to enable appropriate blocking action to be undertaken. The need to virus scan all downloaded documents was detailed in paragraph 13 followed by the requirement that virus problems were to be reported to IT support staff.

The next section explained the policy of placing orders over the Internet, and the need to comply with pre-existing procedures before doing so. This was followed by guidelines for transmissions, including the formatting of documentation and the requirement that the use of the Internet should be considered only if other methods are unavailable. Finally, the policy stated that laws should not be violated and that activity causing problems to the computer systems in any form was not permitted.
1.2.2.2. Section B – E-mail Services

This section set out the policy for the use of email and the potential problems that could be foreseen by its use. It began by indicating the need for care in composition and that delivery could not be guaranteed, requiring that important messages should be verified with a telephone call. The requirement that inappropriate mail should not be distributed was clearly stated.

There were guidelines regarding the way that email was written, stating the problems of all uppercase and all lowercase writing and its interpretation. The policy stated the importance of clear identification and regular checking of mail.

The final sections detailed the requirement that large email attachments should not be sent, and that senders should consider that the recipient might not have the appropriate software to open it. The policy also stated that attachments should only be opened if from a trusted source. Finally, the sending of bulk or copied email was discouraged.

1.2.2.3. Section C - Internet/Intranet Services

This section further detailed the security aspects of the use of the Internet and Intranet services. This included the maintenance of passwords and logins and the requirement that staff should only be logged on for the minimum amount of time required to complete the task in hand. This section also indicated that computers should not be left unattended, particularly whilst logged onto the network. It also stated that any transactions undertaken by a username would be considered to have been conducted by that person or with their permission, thus placing responsibility on the registered user.
The downloading and installation of software was not permitted. The council also stated its awareness of the problems of time wasting and that unstructured browsing was not permitted. The policy then gave brief guidelines for searching including the use of keywords and the recording of frequently visited sites into favourites.

The problems of large files and the space they take up on the server were discussed with recommendations that such files should not be downloaded if alternative methods were available. Finally, it was recommended that files that may be useful for others should be made directly available, and users should not prompt others to download them.

Although the policy document detailed here was a draft copy, it was immediately apparent that there were some related points that were scattered throughout the document in no particular order. This may lead to users being less clear about acceptable use. It was also suggested by this use policy that the Council did not consider the use of the Internet to be a cost or time effective tool, and was discouraging its use rather than embracing it. This was evidenced by the policy where it encouraged staff to use alternative methods of communication, and placed considerable restrictions on the availability of email and the Internet.

Overall, the policy was reasonable and employees were largely unconcerned about its main points. The only criticism was the very restrictive nature of some elements of the policies which meant that the potential of ICTs may not be realised within the council.

This next section sets out how the interviewees for each organisation were selected and provides profiles for each participant. It then details the interview process for each organisation. This section therefore enables a contextualisation of the research participants prior to examination of the data analysis which appears in chapter 5.

4.3.1. How the Interviewees were Selected.

There were a number of selection methods that could have been used for choosing the participants for this study. Those methods included random selection, systematic selection and purposive sampling (Denscombe, 1998; Blaxter, Hughes and Tight, 1996; Sabbie, 1995; Bynner and Stribley, 1978). However, in this research project, the selection of the participants was subject to some restriction. In the first instance, at Alstec Plc, there was good co-operation with the researcher in the selection of participants, although time was distinctly limited and selections had to be made under some pressure. However, those selected at Alstec were well representative of the demographics of the organisation as indicated in the description of the process below.

The criterion for selection were a combination of age, gender, position within organisation, and length of service. In order to discover individual perceptions, it was felt to be important that there was a reasonable mix of participants based on the mix of individuals within the organisation. Had a purposive sample of one department been elected for example, then the results would have been more likely to reflect the departmental structure and culture rather than indicate individual feelings on the issues.
3.1.1. Selection at Alstec

On arrival at the company, the researcher met with the IT manager who was a key author of the usage policies detailed above. Together the personnel files were accessed to decide upon those who would be invited to take part. The system operating the personnel files was able to sort along certain specified criteria such as by age group, length of service, or alphabetically. It was decided that selection should be based on a multiple of factors in order to gain access to people with a wide range of positions and service history. Individuals meeting each set of criteria were then selected using the blind pin in the list method to avoid any preconceived ideas that could be influenced by the names of the individuals.

Once selected the individuals were invited to participate by email directly from the IT manager’s office. It was explained from the outset that participation was on a voluntary basis and that withdrawal from the study was at the participants’ discretion. All those invited were reassured that the information would be treated with the strictest confidence and only used for the purpose that it was intended, according to the Data Protection Act 1998.

Only one person declined and another employee was selected from the same department who had a similar service profile. At the start of the interview all participants were advised of the nature of the research and further assured that confidentiality would be maintained. Prior to commencement of the interviews all participants signed a research ethics consent form (Appendix II) and questions were answered regarding the process and the research project itself.
1.3.1.2. Interviewee profiles

As all personal identifiers have been removed from the data, individuals are only identified by the use of a letter, which indicates each participant for research purposes but which maintains confidentiality for each individual.

Participant A

Participant A was a mature woman in her early fifties. She worked in the Information Services Group as the Lotus Notes Analyst/Programmer and had one year of service. She was highly qualified holding both a Mathematics and Computing degree. She appeared very relaxed and talkative and had an apparently open manner. Participant A had unlimited access to the Internet at work and a computer at home, which was protected by a firewall. It became clear that she had considerable faith in the organisation’s privacy protection policies and that the user policies were accepted as standard. Participant A was very aware of the possibility of privacy invasion, particularly from the Internet but recognised that some may not be as aware as she.

Participant B

Participant B was a man in his late thirties. Participant B worked in the Manufacturing/Defense department as a Skilled Welder and had over twenty years experience. A time served apprentice with the company, Participant B had no direct computer use in the workplace, but was computer literate, with Internet access at home. A welding teacher at a local technical college, he was also very aware of the potential commercial use of personal information, particularly as his wife worked in that area. Participant B was very interested in being a participant in the study.
Participant C

Participant C was a young woman in her early twenties. Participant C worked in the training Department as a Training Administrator. She had full Internet access at work and access to a computer at home. Although participant C was soon to be made redundant after only four months service, there was no evidence of disenchantment with the company over this. Participant C appeared a little over cautious during the early stages of the interview, perhaps due to insecurity within the job or due to my presence. However, participant C became highly articulate once she began to relax and talk more freely.

Participant D

Participant D was a woman in her mid thirties with one year service. She worked in the payroll department as an administrator. Initially, participant D appeared very nervous and gave yes/no answers to questions. She had full Internet access at home and at work and expressed no particular privacy concerns at the beginning. However, as the interviews progressed fuller responses were given and evidence of a greater degree of concern was indicated by her efforts to avoid junk mail and phone calls.

Participant E

Participant E was a man in his mid thirties with seven months service and who worked in the finance department as a financial controller. He was largely unaware of any monitoring of computer use within the organisation despite this being clearly indicated in the ICT use policies. Participant E expressed trust in the organisation to behave...
thically when dealing with personal information. He was generally unconcerned about privacy issues although showed an awareness of the need to protect oneself online.

Participant F

Participant F was a woman in her late fifties with thirteen years of service, who worked in the Accounts Department as a Senior Accounts Assistant. She had Internet access at work but no computer at home. Participant F was largely unconcerned about privacy protection within the organisation, which she considered was possibly due to her retirement within the following three months. Participant F was very unaware of the potential for privacy abuse due to the increase in computer use, but was interested in discovering more now her awareness had been raised.

Participant G

Participant G was a man in his mid fifties with ten years of service. He worked in the defence systems department as a proposals engineer. Participant G was very aware of the social implications of the loss of privacy. Although he had Internet access at work, Participant G was in dispute with Internet providers at home and so was not online at the time of the interviews. He protected his own personal privacy well, and appeared more aware than most of the uses of personal information, and the need for protection. He was talkative and articulate during the interviews.

Participant H

Participant H was a man in his late fifties with thirty years service overall in recent years as part of the management team in the role of technical director. Participant H
had Internet access at home and at work. He was self assured, informative and concerned to up-date and improves the culture within the organisation. Participant H believed that all staff should be aware of monitoring and the ICT use policies, particularly as he was involved in the formulation of those policies.

Participant I

Participant I was a man in his early thirties with six years of service. Participant I worked in the Information Systems Group as an Analyst Programmer. He had a Computing and Mathematics Degree and had Internet access both at home and at work. He was largely unconcerned about the release of personal information, but had some concerns over Internet security.

Participant J

Participant J was a man in his late twenties with six years of service working in the Marketing Section as a Marketing Assistant. He had a Design Management Degree. Participant J had little concern over the commercial use of personal information, which he saw as a good thing which was possibly due to his marketing background. Personal experience of problems had led to concern of how well the organisation protected his employment details and personal information.

3.1.3. How the Interviews were Conducted.

It was decided that in order for the interviews to be undertaken in a relatively relaxed atmosphere, that there would be two days of interviews in the first phase. This meant that the interviewer had only four or five per day, and could considerably overrun the allotted forty minute slot if necessary. This proved to be useful in that some interviews...
were particularly informative and longer than the initial forty minutes allotted, whilst some were considerably shorter. Alstec provided the researcher with an office and office was which helped to create a more relaxed atmosphere. As the office provided was within the management centre, some of the interviewees however were a little nervous in the beginning, possibly due to the unfamiliarity of the surroundings, and the nature of being involved in a research project.

It was agreed that the second phase of interviewing would be undertaken several weeks after the first phase. This was for several reasons:

- To allow the interviewees to think about some of the issues discussed.
- To minimise disruption of the working week.
- To analyse changes of perception between the two interviews.

The second phase of the interviews took place in the same room as the first and under the same conditions. This enabled the research to be conducted with some degree of control over the environment. The interviewer was careful to wear appropriate smart but non-threatening clothing to minimise the effect that the interviewers appearance may have had on the interviewee.

3.1.4. Selection at Hinckley and Bosworth Borough Council

As with Alstec Plc, the initial contact with H&BBC was made by telephone call and then a follow up letter. H&BBC were also happy to be involved in the research project, seeing it as an extension of their public service ethos. A meeting was set up with the district Secretary.
I&BBC however were more reticent than Alstec Plc in allowing this researcher access to employee lists and insisted on self-selection of interviewees. Interviewees were elected by an employee from human resources using the criteria stated by the researcher to ensure that there were good representations of age, experience and different departments. The intensive Data Protection training meant that the staff was greatly aware of the potential for infringement of the Data Protection Act which was why the researcher was not allowed access to the employee lists.

On analysis of the list of selected participants, it became clear that a good attempt at providing the researcher with a broad and representative group had been undertaken. Whilst it must be considered that there may have been some bias in their selection, it is the belief of this researcher that the selected list was compiled fairly and with due consideration of the original aims of the research project. This is because the study was more concerned with individual perceptions than an examination of the council per se. However, there was awareness that there may have been some influences to which the researcher was not party, that may have affected participant selection, but was out of the control of the researcher. The results therefore, whilst valid for their investigation into perceptions, may have been less so for the purposes of research into the organisation itself.

3.1.5. Interviewee Profiles

As with Alstec Plc, all personal identifiers have been removed from the data and individuals were only be identified by the use of a letter. This indicated each interviewee for research purposes but which maintained the anonymity of each individual.
Participant K

Participant J was a man in his mid fifties with nine months service who worked in the environmental health department as head of department. Participant J had email and internet access at home and at work, but rarely used the computer at home. He felt that the council was about five years behind in its take up of new technology. His department was responsible for the CCTV systems in the local area.

Participant L

Participant L was a woman in her late forties with six years of service. Participant L worked in the council tax department as an administrator. She had a computer at work but no Internet access. She did however have Internet access at home, which she used rarely. Within her job, participant L handled large amounts of personal information. She saw some of the restraints of the Data Protection Act 1998 as directly impacting on her departments’ work thus making some parts of her job more difficult.

Participant M

Participant M was a man in his early fifties with eighteen months service working as the public relations person for the council. He had an old computer at work, which provided internal email and little else apart from word processing and considered I&BBC to be behind in its implementation of computing technology. Participant M had two computers at home, networked and firewall protected. He was very aware of privacy issues and the possible social implications.
Participant N

Participant N was a woman in her mid twenties with two years service who worked in the accounts department as principle accountant. Participant N had a computer at work, but did not have Internet access, just internal email. She did however have Internet access at home. She considered that there was strong transparency of information culture within her department but that this was combined with good privacy protection.

Participant O

Participant O was a woman in her early fifties with eighteen years service working in the benefits office as manager. Participant O had a computer at work with external mail but did not have a computer at home and had no immediate interest in obtaining a computer for personal use. She accessed large amounts of personal information and was very aware of the implications and responsibilities under the Data Protection Act 1998.

Participant P

Participant P was a woman in her mid forties with six years service who worked in the electoral registration department as manager. Although she had a computer at work, she did not have Internet access. Participant P had no computer at home, without any apparent interest in obtaining one in the foreseeable future. She accessed large amounts of personal information and was very aware of the implications of the Data Protection Act 1998.
Participant Q

Participant Q was a man in his late twenties with one year of service as the district secretary with a legal background as a barrister. Participant Q had a computer at work that had both external email and Internet access. He also had a computer with Internet access at home. He was also the nominated officer for data protection within the Council. Participant Q was highly articulate and very aware of privacy issues.

Participant R

Participant R was a woman in her mid twenties with four years of service who worked in the legal department as a legal assistant. Participant R had a computer with only internal email. She also had a computer at home but no Internet access. She considered that the Council tries hard to operate good practice with regard to personal information.

1.3.1.6. How the Interviews were Conducted.

Interviewees in this case were arranged directly with the participants and two days were offered as choices for the initial interview. Once again, the interviewer was provided with a room but no refreshments were provided in this instance. The interviews were scheduled to last for approximately forty minutes. As with Alstec Plc, it was decided to leave several weeks between first and second interview. However, it was rather more difficult to arrange convenient interview times with some of the participants and some interviews were conducted in their own offices. This was largely due to the implementation of the up-dated Data Protection Act 1998 and Freedom of Information Act 2000, which was taking up considerable training hours. There was also a local election occurring during this time, which made finding time for the interviews.
challenging. All second interviews were conducted within three months of the initial interview.

4.4. Conclusion

This chapter has introduced the organisations selected for the research. It has also identified and analysed the ICT use policies in order to ground the research in the cultural context of each organisation. The participants were introduced and their profiles detailed to enable the responses detailed in Chapter 5 to be placed into context for each individual. The next chapter details the analysis of the information gathered during the field study.
Chapter 5: DATA ANALYSIS: A DESCRIPTION AND ANALYSIS OF THE FIELDWORK INTERVIEWS.

This chapter provides a detailed description and analysis of the interviews taken during the fieldwork. This chapter begins by describing the processes that were used to analyse the data gathered during the interviews. It offers an overview of the way that the techniques were used and how this involved the five stages of the research process, identification, capture, (identified in Chapter 3) bracketing (reduction), construction, and contextualisation (described below) as required by the techniques of interpretive interactionism.

The following section describes in detail the analysis that resulted in the identification of important themes. The next section offers an organisational analysis providing perspectives and a public/private sector comparison and then goes on to detail the analysis of two individuals from each organisation. Further analysis of each particular focus, i.e. organisational and individual, enabled conclusions to be drawn that constituted the findings of this research and which is detailed in Chapter 6. This provides answers to the original questions posed at the beginning of this research.

The aims of the analysis were principally to identify:

- The perspectives of the individuals on the importance of privacy at a personal level and at an organisational level.
- To analyse current policy within the organisation.
• To discover the impact of information and communication technologies on perceptions of privacy.

• To discover similarities and disparities between public and private organisational perspectives in their approach to privacy and new technologies.

During the analysis of the information gathered, the focus was on the individual participants the impact of technology and their perceptions of privacy. This meant that the analysis sought to identify perspectives through the eyes of the participants, as they saw it, whilst examining the cultural influences of the organisations they worked in.

The framework for analysis identified in chapter three was seen as a means to assist in the contextualising of the information and to aid in bracketing and interpreting the experiences of the participants. The five key issues of importance, awareness, privacy as a right, the effects of ICTs, and the role of the organisation enabled the responses to be categorised during the contextualising phase of the analysis. The key influences identified in the framework were age, position within the organisation, and length of service. Each constituted a further aid to the analysis in order to locate experiences within the perspectives of the participants. These issues and influences were considered throughout all stages of the analysis.


Figure 5.1 is a conceptual model of the analysis process. It should be noted that the analysis was on-going and in keeping with the hermeneutic circle was incomplete and
ontinuous until the fusion of horizons was achieved. This model indicates the steps taken during the analytical process. Each process was completed several times, for different themes that arose from the data, utilising the perspectives of each of the above-mentioned issues and influences.

Figure 5.1 Analysis Model

Figure 5.1 clarifies the interaction between the elements of the information analysed and does not intend to provide a definitive sequence. All parts of the analytical process were interrelated. The age, position within the organisation and length of service of the objects was considered when reading the text. This was important in order to facilitate
consideration of the context in which the participants were reacting to questioning. During the process of reduction, where themes were emerging, it was necessary to be aware of the original issues as laid out in the framework discussed in Chapter 4. In this way, importance, awareness and so on could be considered for each issue raised. The valuation process is shown surrounding the model, to indicate the ongoing process within the analysis.

6.2. The Steps Taken Towards Analysis.

The following section details the steps taken during analysis. This indicates how, in keeping with interpretive interactionism and the hermeneutic circle, the answers to the research questions were revealed.

All interviews were audio-taped and transcribed into Microsoft Word 7.0 program and printed for backup. The transcriptions were then read and considered in light of the five issues of importance, awareness, role of the organisation, effect of ICTs and right to privacy. The tape-recorded interviews were also listened to repeatedly to discover the nuances of conversational speech which would impact on interpretation of what the interviewees said.

It is often the case that how something is said, the pauses; speed of delivery; stresses on certain words and so on, may significantly impact on the meaning of the dialogue. An example of this is where someone may praise the organisation for its handling of personal information. Analysis of the text only may indicate a high degree of trust in the organisation. Only when the interview itself was listened to, was the sarcasm evident in the tone of the interviewee’s delivery. Clearly, the analysis of the interview
the discovery of meaning in this instance would have been seriously flawed had the
ape-recorded interview not been re-examined.

Although the transcription attempts to include as much information about the interview
as possible, for example inserting dots for pauses, the inclusion of ‘erm’ and ‘laugh’, it
was not possible to fully include the tone of speech in the transcripts. Linguists and
speech therapists that are trained to transcribe using symbolic representations of speech
may be able to include some further depth in the analysis of how something was said.
However, the purpose of the interviews was to provide insight into individual
perceptions of privacy and not to analyse the formation of speech per se.

The first stage of the analytical process involved listening to the tapes as a whole to
discover the flow of the conversation. The tapes were then transcribed into text. The
transcription was undertaken by the interviewer and listened to several times to discover
meaning that was not derived entirely from text and to decipher further any narrative
that was unclear or missed in the initial transcription. Although the hermeneutic
approach was originally developed as a method for interpreting texts, particularly
religious texts, the advantage of having the spoken dialogue served to enhance the
analytical process and to further verify the conclusions drawn.

From reading the transcripts and listening to the tapes, several perspectives began to
merge, these being ideas, opinions and views that recurred often in the dialogue. As
each perspective emerged, the transcripts were re-read to ensure that they had not been
missed in earlier readings and to discover the extent of agreement on the points raised.
In this way, the patterns of meaning and interpretation were discovered.
he main focus of the reading was to consider that each individual was indicating their own ideas and perceptions of privacy in the context of their lived experiences. The interpretation of each interview had to consider that it was the participants’ interpretation of the issues that was being investigated, rather than the discovery of generalisable opinion that could be attributed to a wider population. However as many of the participants had very similar perspectives on privacy, personal information and so on, the research was able to provide insight into the perceptions of individuals within the particular environments being studied.

As perspectives emerged, they were identified as a heading for further analysis. Then all the dialogue that had mentioned or considered that particular issue in the same context was copied and pasted to a separate document. In total, seven key issues were identified for further analysis:

- The importance of Privacy.
- Awareness of the Issues.
- Access to Personal Information.
- Data Matching.
- CCTV and Surveillance.
- The Role of the Media.
- Age Considered Perspectives.
These issues were revealed as important to the participants, and were seen as critical to revealing individual perspectives of privacy during the enquiry. By discovering the participants’ views and opinions on these issues, an overall picture of privacy perception within the constraints of the research questions was discovered. The revelations, experiences and interpretations are highlighted by direct quotes (shown in italics) from the participants. In this way, their stories are told from their perspectives and within their own context.

3. Data Analysis: A Description and Analysis of the Fieldwork Interviews (Organisational Perspective)

This first section of the analysis deals primarily with organisational perspectives. This means that the main purpose of the analysis was to reveal the interaction between the organisation and the individual. Two research questions in particular were investigated during this part of the analysis. Firstly it was revealed how individuals within the organisation perceived the issues of privacy and privacy protection at an organisational level. Secondly, how the organisational culture had affected and had been affected by the individuals within it. Whilst it was expected that this stage of the analysis would also provide insight into the other two research questions, those findings were utilised in later analysis of individuals.

3.1. The ICT Revolution.

At the first instance, it was necessary to discuss how the advent of ICTs had affected individuals within the organisations. The first part of the analysis therefore was to study these effects, to identify the perspectives and feelings of the participants and to relate
stories of their experiences of the computer revolution. In this way, by discovering the impact of computers it was possible to ground the information within the cultural context being examined. The deconstruction of the conversations to reveal the perspectives of the participants was able to shed light on individual perceptions of privacy within the organisations.

This section therefore examines perceptions of privacy and computer use from an organisational perspective. Individual perceptions are examined within a workplace context and consider the organisational perspectives on privacy protection and computer use. Attitudes of the participants towards organisational policy are discussed as are the attitudes of the organisation towards employee computer use and privacy protection.

Each organisation is examined in turn and then comparisons are drawn.

3.1.1. Hinckley and Bosworth Borough Council.

The first issue to be considered regarding the ICT revolution was how it had affected the way that the organisation behaved and operated. In the case of H&BBC it appears that there had been a relatively slow take up of new technologies resulting in it being seen to be falling behind some other public sector organisations. A participant who had been working for some years at a different council, which had embraced new technologies sooner and more rapidly, noted this. What was unclear and not examined during the interviews were the policy reasons for this late implementation. It could be that there was a lack of resources, political will or even perceived need. Whichever the reason, it meant that decision makers within the council had a cautious attitude towards the new technology which had led to a policy of firm control. This culture had resulted
management regarding computers, email and the Internet as a privilege rather than embracing the technology as a tool.

The future expectations for ICT use within government organisations however are for continued expansion of services. This had been actively encouraged by central government with e-government initiatives being considered a priority. In view of this, it was expected that H&BBC would continue to implement new technologies into the working environment. It was also hoped that as they become more familiar, there would be a relaxation of some of the more restrictive limitations of its use. Once it was recognised that some flexibility was acceptable providing abuse did not occur H&BBC should be able to use the technologies with less concern and possibly greater effectiveness and with a higher level of trust in its employees.

All interview subjects from Hinckley and Bosworth Borough Council had undertaken data protection training in house, prior to the initial visit. Few of the interviewees were in the external email system, but they were expecting to have access by the time of the second interview. The value of this time scale can be seen as an opportunity to identify the effectiveness of the training and the importance felt by the interviewees of the need to comply with the data protection legislation.

At the time of the first interview, all participants had completed the training as little as one or two weeks prior to the interview. The issues and rising of awareness were therefore very new and fresh. The subsequent interview, being conducted two to three months afterwards, enabled the impact of the data protection training and the presence of the interviewer to be discovered after the initial intense awareness raising experience.
The second interviews were conducted when the new guidelines and email use
document had been implemented. This enabled observation of how the interviewees
had become accustomed to the daily use of the procedures, and how well it had become
embedded and accepted within the culture of the organisation.

3.3.1.2. Alstec Plc.

In Alstec Plc, all except one of the participants had open access to email and the
internet, which had been embedded within the organisation for some considerable time.
The impact of ICTs therefore had gone beyond the initial change to a point where
acceptance and reliance on both the computerisation of the systems and the use of the
internet had been established.

Data protection, unlike within H&BBC appeared to be of little importance to Alstec
employees. This may have been largely due to the lack of training within the
organisation. This was identified as a problem by employees as was the insufficient
training for new members of staff. At Alstec Plc computer training was very much ‘on
the job’ with problems being addressed directly to the technical support staff. This was
seen as a distinct lack within the organisation at the highest level and staff development
was being considered a priority by management at the time of the interviews.

For clarification purposes, this section identifies each area of examination separately,
and considers how they related to individual perceptions of privacy at an organisational
level. Below is an analysis from an organisational perspective and examines the
public/private perceptions of privacy and ICT policies within those organisations. An
n-depth description of the organisations and the participants can be located in Chapter 4.

6.3.2. The Importance of Privacy

The importance of privacy to individuals is a key component to the development of privacy policies and practice both currently and in the future. This is because if privacy is not important then it may not matter if it is not protected. However, as identified in Chapter 2, the importance of privacy is not in doubt. It is the scope and extent that privacy is important that is being investigated here. The research showed some considerable agreement between the participants on the issues of privacy and its importance particularly in an organisational context. There were several influences such as age, position within the organisation and length of service that had affected the sense of importance felt by the participants.

In the whole, the participants at both organisations were in agreement that privacy was important to them; I actually rate it quite importantly... If I say something in confidence expect it to be kept in confidence (Participant A). This was particularly noticeable with regards to the distribution of personal information and was considered in light of the organisational policies for protecting employee and consumer privacy. Participant A stated that people shouldn't have access to things they shouldn't and participant D considered that just knowing that the information is secure, where you think it should be as important. Others were particularly concerned with the surveillance aspects of privacy; I suppose the ability to do what you want without being watched...
more than anything (Participant A). Privacy with regard to workplace surveillance and in particular the use of CCTV monitoring is considered further below.

Participant K offered a good example of the opinion of many of the participants with regard to the importance of privacy when he stated;

'I'm not so concerned about the usual information, my name, address, telephone number you know, date of birth, and usual sort of information. But... when it comes to very private, personal information, I wouldn't want that to be known to people who don't legitimately need it.

What this indicated was that individuals were not too concerned about the privacy of general information. They will share names, addresses and other personal identifiers such as date of birth, seeing this as necessary to participate in society. One participant commented that, what would be nice is the opportunity to say... I don't agree with this society, I'm going to go and live on a little Scottish Island. This comment was made in the context that participation would require some co-operation with requests for personal information and to try to avoid it was seen by the participant as unrealistic. It therefore shows that there was some acceptance with these demands for information even though the lack of real choice in the matter was viewed with concern.

These sentiments were echoed throughout the entire group of participants from both organisations. When the importance of privacy was considered based on the age considered analysis there were few striking differences, although some subtleties were evident. Those from the older age group tended to consider that privacy had been lost.
to some extent particularly with regard to information available to organisations and people whom they did not know.

*All sorts of people hold information on us, whereas previously it would have been relatively few people* (Participant K).

However, there was also acceptance that privacy of personal business to those around them was somewhat less in the past, when neighbourhoods were more closely knit, and communities often comprised large family groups in one area. This change in the make-up of communities had been more greatly noticed by the older participants and who considered that although there was less privacy in some areas, there are more in others; *I think you know your neighbours less and less and people perhaps couldn't divulge information that they used to be able to in a small community* (Participant P).

It should be noted, that the younger participants were also aware of this change in community, perhaps due to being told of the change by older friends and family or memories of childhood. However, the comments often appeared to be those of someone who had been informed of the change rather than someone who had experienced that change personally; *I would say more people know about you than would have done many years ago* (Participant I).

Where there was a consideration of the position and length of service of the participant within the organisation, it was clear that there was little difference in degree of importance felt. It was noticed however that those with a higher level of authority within the organisation tended to be more aware and more articulate about the issues
han those with less responsibility. This may have been due to either a higher educational level or that a greater degree of awareness was considered necessary for their position. The participants may have been nervous about being involved in the study due to their familiarity with the process of interview and presentation. This may have made participants more relaxed and therefore able to articulate their thoughts more clearly than some others.

As has been discussed in Chapter 2, privacy is subjective, with problems of definition, degree of importance, legislation levels, and other distinctions, which make privacy as a concept difficult to pin down. One aspect of privacy that created the main area of confusion for many individuals was surveillance. This issue produced an immediate dichotomy, with some individuals initially indicating a lack of concern or importance given to surveillance issues and its potential impact on their privacy; *It doesn’t bother me cos I don’t think I’m being watched any more than anybody else* (Participant D) who later stated, *I don’t suppose I would like it when I didn’t know it was happening and I didn’t have any control over it* (Participant D).

Later, there was evidence of this same individual actively taking steps to protect her privacy by removing her name and address from the telephone directory. Participants further contradicted this initial claim with examples, caveats and exceptions such as requiring permission or at least the information that surveillance was being undertaken; *do anything you like as long I agree to it, as long as I know you are doing it* (Participant I). This confusion felt by D was evident in many of the participants. Many people were happy to be under surveillance for crime protection purposes, and to have their
ames and addresses known. However, it was also considered that this same
formation should be protected or at least only distributed with permission.

The most commonly uttered phrase with regard to surveillance was; *if you are doing
nothing wrong, it doesn't matter*. This, and variations, were stated by many participants
during the interviews. There was a general acceptance of the need for surveillance,
particularly in the streets where the presence of CCTV was becoming an everyday
occurrence in the UK and seen as important for crime prevention.

One of the key concerns regarding CCTV was its effectiveness. It was fortunate that
one participant was the head of the department directly responsible for the CCTV
ameras in the Hinckley area. It became clear from relatively early on in the analysis
that a high degree of importance was placed on the use of CCTV. This does however
seem to be in contrast to the actual usefulness of such systems with the interviewee
supporting the view that CCTV leads to displacement of crime rather than prevention of
crime.

This clearly shows how perceptions of an issue can be affected by the type and extent of
knowledge of that issue. There has been some concern (Webster, 1998, 1999; Brown,
995) as to the lack of public debate, and the one sided approach of authorities, bringing
about the use of CCTV. Although this is entirely a different debate from that of this
thesis, it is of interest in highlighting the need to raise awareness through open and
conest information provision.

3.3. Awareness of Legislation, Policies and the Organisational ICT
ulture.
Low aware individuals were about the issues surrounding privacy and the impact computing technologies had on their perceptions was also a key point in this study. It was during the initial interview stage in particular, that the awareness of issues came to the fore. The first and most noticeable conclusion drawn by this study was that the employees of Hinckley and Bosworth Borough Council were far more aware of the issues of privacy than those at Alstec Plc. This was chiefly because they had been undergoing some intensive data protection training and were therefore thinking of those issues in advance of the interviews.

There were employees at Alstec who were very aware of the social aspects of privacy, and surveillance, but no-one interviewed had anything more than a very vague knowledge of the Data Protection Act 1998. This was despite some of those interviewed being involved in the collection of personal or sensitive information such as payroll details. A lack of training within Alstec Plc, which was accepted by senior staff members interviewed as being problematic, was probably chiefly to blame for this, combined with a belief that the Data Protection Act 1998 did not really apply to them in any major way. For this reason, this next section of the analysis has been separated into sub-sections.

The first part considers the awareness of Alstec employees to the Data Protection Act 1998 and the internal ICT use policies of the organisation. The second part considers the same aspects of awareness from the perspectives of the employees at Hinckley and Bosworth Borough Council. A conclusion then considered the extent the differences in awareness of these documents had affected the privacy perceptions of the two groups. An in-depth analysis of the policies is set out in Chapter 4). The analysis then
considered awareness of the issues on a more personal level. Once again this was dealt with separately, from the perspective of the employees of Alstec Plc and those of Hinckley and Bosworth Borough Council. This analysis therefore highlights the key issues and areas of concern that reveal the awareness of the issues for each group.

3.3.3.1. Alstec Plc.

As previously stated, the employees had little knowledge of the Data Protection Act 1998 beyond its actual existence; well I’ve heard of it but I don’t know very much (Participant F). The Act was considered to be of little importance and relevance to them. An example is that D did not consider data protection knowledge to be relevant and yet had access to sensitive personal information due to her work in the payroll office. When asked if she was aware of the details of the Act, she replied not really. Because really all the information we get is a clock number and an amount. This lack of importance no doubt was borne out by that very same lack of knowledge of the Data Protection Act 1998.

Two months prior to the first interviews, all employees had been sent an Internet Use Policy and an Email Use Policy by email. It was immediately clear that little interest had been taken in the details of the policies by the staff. When the policies were discussed with the participants, there was a good awareness of the broader implications of the policy. However, many had not read the policies in detail, presuming that they were reasonable, sensible and requiring little consideration. Many employees had not read through the policies stating that Its just straightforward really I would have bought, I haven’t obviously read it all, but its like anything just don’t misuse it (Participant D). Others had just glanced over them; I’ve quickly scanned through them.
Participant J). This lack of interest in the policies set out by the organisation for the use of email and the Internet may have led to some abuses of the system. However, having considered this, most of the participants were confident that the policy would be sensible and were, by and large, adhering to the policy through common sense and respect for company property and reputation.

Although there had been some abuses of the system, this was not considered to be a major problem by senior staff, as it had been minor and dealt with intra-departmentally. All employees had been informed of the detection of the abuse via email, as this was considered by senior staff to serve as a warning to those who may have considered abusing the system in the future. Widely publicised and severe methods of disciplinary action such as the sacking of 40 employees by Orange in September 2000 (Wakefield, 2000) were considered too severe and unreasonable and as one senior employee indicated I don’t think that the sort of draconian approach that some companies have made in terms of booting out twenty people because of something is gonna do any good (Participant H).

There was an indication that some employees were unaware of the monitoring of the internet use by the organisation; I am not aware that there is any monitoring (Participant E) despite it being explicit in the usage documentation. This employee however, had not read the use documents and had presumed they were the same as his previous company; It hasn’t affected me at all... the last company I was at had similar notes and policies (Participant E). This explains why Participant E had not discovered the section regarding Internet monitoring.
In general, the ICT use policies of the organisation were not read in any great depth, but were expected to be sensible and therefore easy to follow. The policies allowed some personal use provided it was only during non-working hours such as lunch breaks, and did not involve downloading music or inappropriate material.

Perceptions of the organisation from an employee perspective were mixed. There was a high level of trust in the organisation to protect personal information, which was not borne out by the level of security experienced by some participants. The re-organisation of the company after the management buy-out had created some uncertainty and the introduction of updated servers and computers had led to some potential breaches of security where information was easy to access; we've just changed over to a new file server, and information was being routed across into areas that were common domain areas where they probably shouldn’t have been (Participant G). However, it appeared that these loopholes were being tightened, while the old system was being decommissioned and the new one brought online. There was also some concern that certain procedures were insecure, allowing for sensitive information to be seen by inappropriate members of staff; If we are off sick, it then goes to a local administrator and she keeps the details of medical statistics just on a database, so that’s not that secure... there’s no reason for administration secretaries to know why I've had time off (Participant J). It may be that there were other personal information security concerns that did not come to light during the interviews. Participant J was concerned due to its relevance to him, whereas others may not have had any personal experiences and so remained unaware of any potential internal security problems.
In contrast to participant J, the majority of the employees of Alstec felt that the company protected personal information well, and that staff with access to that information undertook to maintain security; *I think it's strictly confidential... I know that no-one round the site has access to that type of information* (Participant I). *The information I don’t need I can’t see* (Participant C). It was also clear that personal information was not given out or shared with any other organisations; *the information we keep here is purely for our own business* (Participant H). Access to their personal records to ensure that the information contained within was correct was available to all employees; *It is open to anybody... to see what information is on them* (Participant H) therefore maintaining compliance with the Data Protection Act 1998.

To conclude, the participants from Alstec Plc were largely ignorant of the Data Protection Act 1998 principles but were aware of its existence. They were uninterested in the usage policies of the organisation, which led to some participants being unaware of the monitoring being undertaken by the organisation. However, all were aware of the principles of fair and reasonable use of the Internet and email facilities, and were happy to comply with these. There was some concern regarding the security of personal information within the organisation, and some sensitive, although not necessarily personal information had been insecure during the change-over process from the old to the new system.

Overall, the level of awareness of the employees regarding the Data Protection Act 1998 was poor. Their awareness of the usage policies was adequate but not detailed and their perception of security of personal information at an organisational level was, on the whole, one of trust in the organisation to behave ethically. However, it was recognised
that minor security flaws existed. Awareness of sociological issues of privacy such as
the use of CCTV monitoring or access to consumer information was fairly good but
included some gaps in knowledge of the extent that this information could be abused.

5.3.3.2. Hinckley and Bosworth Borough Council.

As previously stated, the employees of H&BBC had all undergone an intense and very
recent period of Data Protection training prior to the first interview. Clearly this had a
considerable effect on awareness of privacy and data protection particularly at an
organisational level. Awareness of the Data Protection Act 1998 had been considerably
raised due to the training undergone. Prior to this, the level of compliance and
awareness had been relatively erratic; Before the new one came in, they didn’t give us
very much training on it and it was very much hit and miss (Participant P). I think data
protection, when it came in 1984 ... had a low profile and has had a low profile across
the council for the last 16 or 17 years (Participant Q). However, the updated Data
Protection Act of 1998 and the introduction of the necessity for compliance for paper
records as well as for electronic records had raised its profile. Individual compliance
and awareness was very high, with participants being keen to ensure that its principles
were adhered to; We are well aware of what the data protection rules are and that we
need to comply with them (Participant P).

Some of the senior staff felt that there was now an over-zealous approach to compliance
with the Act, and that the training had actually frightened some people into maintaining
a level of secrecy and security beyond reasonable levels; Our chief exec likes to send
birthday cards to people, well he can’t get access to somebody’s date of birth unless
they specifically say he can have it now and they sign something ... I think that’s taking
that step too far (Participant P). The reason for this may be due in particular to the
realisation that individuals can be liable for inappropriate disclosure as well as
organisations; The possibility that people individually can now be taken to task over it
is well as us as an organisation ... that has really made people clam up (Participant Q).

n general though, the introduction of the Data Protection Act 1998 and the training
undergone by the employees of the council had made people more aware of the need to
protect personal information and be more cautious about what they reveal. Participants
were also aware that the training had raised their awareness of the issues; I'm more
careful about what I write after that course (Participant R). The training had also
highlighted the need for security of the information not just its disclosure; it's made me
think about how I should protect that information (Participant N). There had however,
seen a long standing culture within the council of non-disclosure, which had been
strengthened by the impositions of the Act; as a council, we've quite a strong tradition
of not disclosing anything unless we've really had to (Participant Q).

The use of email and the Internet within the council however, was strikingly different
from that at Alstec Plc. Firstly the council was seen to be lagging behind the times in
the take up of new technologies by a significant number of participants, with comments
made such as the whole council system is antiquated (Participant M). When asked if
they considered the council to be behind others with regard to e-government,
participants felt that this was the case and that, I would say, thinking where we were at
the authority that I came from, in terms of one stop shops, kiosks, I would say about 5
ears or so (Participant K).
The concerns articulated above were reflected in the strict email and Internet use policies that had been introduced at the same time as the majority of council office employees were provided with external email, and when some were given Internet access. The policies, in contrast to those of Alstec, and to those of more technologically advanced councils, were seen as harsh, draconian and inflexible by those staff that had experience of a more liberal stance. The policy stated that there would be no personal use of the email or Internet system at any time. This was explained as a way of ensuring no grey areas. Employees were expected to read and sign the use document before being given access; before they are actually allowed to use the system they have to sign to say they have read and accept the terms of it (Participant Q).

There were two main reasons given for the blanket ban on personal use, firstly; because we are a public service then that is one of the reasons that we wouldn’t be allowed to use it for our own purposes (Participant Q) and secondly; it is much easier to police if you say absolutely no personal use (Participant Q). This approach had caused some disappointment, particularly from those employees that had seen a more flexible policy at their previous workplaces; the group that were looking at this were very clear that it was for business use, and in some respects I think that’s a shame (Participant K). Despite the policy, there had, like Alstec, been some minor abuse of the system, where someone had been disciplined for receiving and distributing a joke email. They were disciplined because not only was the material seen as inappropriate but; it was a bitutting edge (Participant Q). It was chiefly considered inappropriate because it was not work related; it was receiving something from outside the council which was irrelevant to what the council does (Participant Q).
The participants felt that the council protected personal information well. There was some concession particularly during the first interview that on occasion information was not secure; *all my budget files are passwords protected in excel on spreadsheets, but I just admit they are all printed out and in a file in a cupboard. (Not locked)* (Participant J). However, by the time of the second interview and the subsequent strengthening of the security ethos within the council due to the training, staff showed considerably more caution; *I've now got all my files in a lockable cabinet,* (Participant N). Since the data protection training, staff had started taking the issues of security much more seriously, and this had been reflected, not only in the way that sensitive or personal information from the customers was treated, but also how internal information was protected.

As stated earlier, with the example of the birthday cards, there had perhaps been some overzealous interpretation of the principles. There was some frustration with the dissemination of information between departments and with other service organisations such as the electricity company. This had created difficulties for some departments; *in the past we could have shared the information with say the electricity board, we could help each other, but we can't do that now* (Participant L). In these circumstances, the new Act had made the tracking of people who had absconded without paying council tax much more difficult.

The Freedom of Information Act 2000 was a piece of legislation that had particular relevance to the employees of H&BBC as it was related directly to public sector organisations. There was some discussion about the general public, some of whom had recently become aware of the right to access their information through the implementation of the Freedom of Information Act 2000. However, at the time of the
second interview, there had been only three requests for information under the Act from members of the public; *having had no complaints or requests at all in the last fifteen ears or so, we've now had three in as many weeks* (Participant Q). There was clearly a potential for a great deal more work should a lot of people decide that they want to see everything that the Council holds on them; *... its going to be interesting to see how the attitudes around the council as a whole develop* (Participant Q).

To conclude, the participants from H&BBC were all very aware of the Data Protection Act 1998 and its principles and were actively seeking to ensure compliance. There was a high level of trust in the Council to protect their personal information for the reason above, and because of the trusting ethos within the council itself. There was perhaps a little over zealous behaviour regarding compliance. This may have been due to the relative newness of the full implementation of the Act and the data protection training, which had created some fear and made the issues high profile. Whether this would continue in the months and years ahead would remain to be seen. With regard to social awareness, the participants at H&BBC were a little more aware of potential abuses of privacy, and yet, like those at Alstec, did not see CCTV monitoring to be of concern unless it was in the workplace.

With regard to the email and Internet use policies, all participants were acutely aware that no personal use was to be permitted, and that there would be some form of disciplinary action for those found to be abusing the system. This was seen to be draconian, and yet fair as the equipment was provided with taxpayers money and not from private resources. However, as other councils have implemented a more relaxed
approach to the use of email and the Internet it was hoped (Participant K), that H&BBC would relax its attitude towards its use in the future.

3.4. Alstec and Hinckley and Bosworth Borough Council – Conclusions

The issue of awareness that has been discussed in this analysis has highlighted several contrasts within the culture of the two organisations studied. It immediately became clear that there was a much higher level of awareness of the Data Protection Act 1998, and the Freedom of Information Act 2000 in the public sector organisation. This was due in part to the public service ethos that has been ingrained within the council probably since its inception, and the recent training undergone by all staff. The need for public sector organisations to be seen to comply with the law was seen to be as great as its actual need to do so.

The private sector organisation had two main reasons for this not to be the case. Firstly, there was little public accountability of its actions beyond its public limited company status, and secondly, it held little personal or personally sensitive data. In fact, within Alstec, the only personal data held was directly related to the personnel and wages information of the staff working there. H&BBC however, being a borough council, held a great deal of information on the local population including council tax records, hackney carriage licence information, criminal records of publicans, and electoral registration information. It became clear that there was a need for the personnel and wages staff at Alstec to become more aware of the Data Protection Act 1998, in order to ensure compliance with the law.
Trust within the organisations that they would protect personal information was relatively high in both cases. Some Alstec employees were unsure as to the strength of security, H&BBC employees however were confident in the security levels at the council.

With regard to the use of the Internet and email, here there were also some stark contrasts. Alstec was rapidly moving forward technologically, allowing all office staff unlimited access to online resources, personal use in their own time, and a flexible approach to its ICT use policies. Some participants however, were unaware of the monitoring in place and so awareness in these areas could be improved. H&BBC however, were considered to be lagging behind in the take up of new technologies, only recently getting external email and providing Internet access only to some key staff. The strict requirement that there should be no personal use of the ICT resources combined with the monitoring of email had served to highlight management concerns about the potential for abuse of the system. There was also some indication of a higher level of caution due to the relative newness of such technologies within the council.

A further study of the policies and attitudes of the council regarding the Internet in particular would be of interest once its use had become fully embedded into the daily working routines of the council. There was no indication during the study that there would be any relaxation of the strict policies in the future.

In conclusion Alstec needed to make greater efforts to raise awareness in order to comply with the Data Protection Act 1998 and to ensure that employees were clear about the ICT use policies and monitoring. The culture within the organisation was
such that trust and flexibility was key, with a technological drive forward being evident within the organisation. H&BBC however, although also operating with a high degree of trust, were more rigid in their application of rules and regulations, which ensured compliance, and awareness of the issues. There was concern however about the lack of flexibility, which could negatively affect the use of new technologies in the future.

5.3.5. Awareness of Current Privacy Threats and Issues.

This section of the analysis will once again take both organisations together. This is because there were surprisingly few differences in the social awareness levels of the participants, even when the extra training of the participants from H&BBC was considered. The issues that are analysed here, were impacted by those discussed above, but are more concerned with social aspects of privacy awareness. They involved consideration of the potential for social control by governments, the extent of commercial data holding, data matching, CCTV, workplace surveillance and the role of the media as perceived by the participants.

5.3.6. Access to Personal Information.

It was clear from the interviews that most of the participants were aware of the potential for abuse of their personal information, and had strong feelings on sensitive information; *people can abuse other personal details but if you send financial stuff through, it's writing a blank cheque and just leaving it on the table* (Participant Q).

In many cases, 'concerns' were not always voiced as concerns, but more often as annoyances or irritations; *with the amount of junk mail I get, I think it should be made...*
illegal...I see it as a massive annoyance (Participant M). This was a particularly strong theme throughout the interviews with concerns and irritation over unsolicited mailings, and commercial access to phone numbers and addresses. Surprisingly, very few of the participants from either organisation mentioned or were concerned about Spam emails explicitly. One participant merely changed email addresses whenever it became too great. You can just lose one and get another one. It doesn’t take much (Participant D). The issue of Spam therefore was considered in the context of junk mail and not considered separately.

In the first interview, each participant was asked what they perceived privacy to be and what aspects of privacy they saw as being of concern to them. This was in order to discover the awareness of the participants of the issues of privacy, what it actually meant to them and which issues were causes for concern. By asking this question during the first and second interviews, it was possible to discover the awareness raising influence of participation in the study and consideration of the Hawthorn effect.

Privacy as an issue was important to all of the participants, but in varying degrees. When asked about privacy of personal information most participants considered that only relevant information should be seen; nobody else needs to know my medical records unless I authorise them to do so, (Participant P). Further, privacy was considered synonymous with security; just knowing that the information is secure, where you think it should be (Participant D).

The most immediate and common response to the discussion of personal information issues involved its commercial use and the receipt of unsolicited mail through the post.
Many of the participants actively sought to reduce the quantity or at least improve the quality of the mail sent to them; *I always tick the box, on anything to say I want the data protected.* (Participant N). However, junk mail was largely seen as an annoyance rather than a privacy infringement; *I got fed up with all the post coming in that I didn’t want* (Participant L). To some the main importance of privacy is in the home; *an Englishman’s home is his castle, nobody has any right to come into your home or disturb your peace or property, so that’s your privacy* (Participant M). Others admit that there was a great variation in what they considered to be private and what was or was not of concern; *I admit I’m always very careful what I fill in and the information I give. There’s certain information, I wouldn’t care who has it, but... anyone that’s got information about me should be able to justify why it is held and what use they intend to put that information to* (Participant K).

This statement is a good example of many of the participants and how they expressed their concerns over privacy. Many of the participants were fairly careful about the information they gave to third parties. Some information however was seen as of little concern, such as name, addresses or telephone number. What most participants saw as important however was not so much who holds the information, or even the kind of information (depending on the circumstances) but the use it was put to. Participants also felt that there was a need to ensure that any use was with consent and fully justified.

6.3.7. Data Matching.
In the area of data matching there was a considerable diversity of awareness discovered. At Alstec Plc, many individuals were unaware of what data matching actually is. This was explained to the participants so that they were then able to assess their perceptions of the principles and potential. Whilst this involved raising awareness in some cases by the interviewer, it was considered necessary in order to gather perception information. Once the participants had considered the uses of data matching there was initial surprise; *I had no idea it went so deeply as that* (Participant F), followed by a general agreement that it is in principle at least, a good idea and should be continued. Many individuals were largely unconcerned by the potential use of data matching, and considered it to be a good way of uncovering fraud and criminal behaviour; *I just think that these are targeting techniques that authorities should be using, to be more efficient in terms of cracking down on crime* (Participant E).

Some concerns were raised regarding the possible abuses of the system and the possibilities for miscarriages of justice or problems with profiles being based on where someone lives rather than on their personal history; *If I lived in the wrong area... then I would be more likely to be accused of something I haven’t done because of that,* (Participant D). However, on the whole, the participants were happy to have their profiles used as an aid to the investigation of crime, citing the ‘if you are doing nothing wrong it doesn’t matter’ adage, as a form of protection against wrongful accusation: *If I’m selected on a target list I’ve got nothing to hide I’m quite happy if somebody was to investigate because of that and then find there’s nothing wrong, that’s fine... I just see those techniques as targeting techniques really* (Participant E).
There was however some concern about the problems of the techniques being only able to give a small piece of the whole picture of someone; its partial information (Participant G). It was also considered that continued and expanded use of such techniques should be carefully considered; I think it’s got to be a... social decision as to whether you want it to be taken that far (Participant G). The awareness of data matching therefore from Alstec employees was minimal, but once that awareness was raised, there was a diversity of opinion regarding its effectiveness and acceptability.

H&BBC participants however were even more diverse in their reaction and awareness of data matching. Some of the participants were very aware of its use, and were actively involved in data matching in order to prevent social security fraud; there’s data matching that we do for the DSS and data matching that we do for the Audit Commission. (Participant O). Again, it was generally considered to be a good way of catching fraudsters such as those who made multiple social security claims. Those involved in data matching considered it to be a valid way of preventing fraud as well as catching fraudsters; As far as benefits are concerned... I’m quite in favour of it... we are there to prevent fraud as well as detect it (Participant O). The future increase in data matching techniques within government organisations was expected to affect work within the council with the expected matching of Inland Revenue files to council files shortly to be implemented. However, a participant who had been subjected to data matching by a credit company and had been refused had very different views from those who had been unaffected by the process; I was refused something, I think it was only like a catalogue or something and I was that annoyed about it that the bank said I could do this credit search to find out what was on my name. It was on my address, because my father had a couple of county judgements that had been cleared. I think even in this
case it was something like 5 years old and that had stopped me from getting credit. So I found that very annoying and also he perhaps didn’t want me to know about it (Participant N).

Further issues such as the ability to personally credit check ones’ address is also of concern, where the credit history of previous or other residents would be provided by the search. In this case the privacy of N’s father had been compromised and his record had directly impacted on participant D’s credit rating.

There was also concern particularly by participant O that some matching was being undertaken that was deemed inappropriate. In this case the employee payroll information was being matched with other databases in order to discover student grant fraud. What concerned participant O was not only that the information was being matched but that no one had been informed of the process. Participant O felt that this was so unacceptable that she had registered a formal complaint about this particular form of data matching; *If you are going to have your payroll details matched and the tenants are going to have their details matched against my benefit records, to make sure that I’m not paying someone, then they ought to be informed* (Participant O).

What mainly concerned participant O was the implication that council employees were more likely to defraud the council than others were. This was clearly in direct conflict with the culture of trust that was generally inherent within the council and could ultimately lead to a souring of relations between employees and employers. At the time of the interview, the results of the data matching had not been released, but the
participant was considerably unhappy about the lack of informed consent during the process.

This sentiment was echoed by another participant who was unaware of the matching that had taken place but who, had they known, would have been considerably upset by it; if they are matching all your personal details and they have access to that when there's no need for them to do, then I do disapprove of that, I do think they shouldn't be allowed (Participant P). The evidence indicates a lack of awareness by the council employees as to the extent of data matching and the data matching of their personal information. When this was combined with the strict email and Internet use policies of the council, it appeared that the level of trust in employees was actually lower than initially thought. The draconian or at least punitive measures in place to control Internet and email use, access to resources and to some extent, behaviour was evidence to show this. However this was in contrast to the working culture within departments, where trust was considered to be high. In comparison, Alstec Plc showed a high level of trust in its employees to behave appropriately, which was an indication of considerable culture change since the management buy out.

There was concern therefore that the employees of the council were trusted less and therefore more restricted than those of Alstec, and they are not informed of some of the areas where they were considered less trustworthy. Throughout the research interviews consent and information were seen as key to acceptability. This was true of personal information dissemination and was also true of CCTV and monitoring which is considered in more detail below.
5.3.8. Closed Circuit Television and Monitoring.

When participants were asked about the use of closed circuit television (CCTV) and monitoring, there was a similarity in the awareness of the potential and nature of its use in both Alstec Plc and H&BBC. Immediately evident was a lack of concern over surveillance cameras and CCTV, particularly in the street; *I see it there as a protection rather than an intrusion* (Participant P). The use of CCTV was considered by the participants to be on the whole, a positive crime prevention strategy needing little justification. However, the use of CCTV cameras in the street was seen, particularly by older participants, as a reflection of the way society had developed; *it’s very difficult, there’s a different culture to what there was years ago, and a lot of things going on. The only way you will actually spot the culprits is through that* (CCTV cameras) (Participant O).

However, the one or two participants with greater knowledge of the way CCTV was operated showed a considerable difference in opinion. In these cases, as in the case of the other participants, the usefulness of the CCTV cameras in principle was accepted. However, their actual use and effectiveness in their present application was of concern; *I’m a magistrate, I sit in court once a month. I have never in 10 years had any CCTV evidence put forward* (Participant M). The problems of displacement were also considered to be of concern to the more aware participants; *they put them* (CCTV cameras) *up in Earl Shilton and the crime’s appeared in Barwell, so the cameras are now going up in Barwell* (Participant M).
Displacement of criminal behaviour was not considered by many of the participants. It was revealed that public knowledge of the problems of displacement in the area was actively discouraged; I've had to politely suggest that comments are not put in press releases (Participant M). A question then is whether the problems of displacement should be revealed to the public? The two areas of transparency and openness on the one hand, safety and security on the other become relevant here. In our society, we have come to expect some accountability for the expenditure of our tax money.

Although there have been many instances over the years of money wasted; the principle still holds that the aim is towards accountability for actions.

Despite the lack of openness with the public about CCTV displacement and its lack of use in court, there was evidence that some participants were already becoming aware of some potential problems; if the camera doesn’t cover that particular area, they can get away with it (Participant O). If the public becomes more aware of displacement and other problems such as consistently low monitoring of cameras, poor quality film, lack of its use as evidence by the police and so on, then the cost of implementation could then be considered too great in comparison with the true social benefits that they bring; so whether in the full analysis you actually benefit, I don’t know (Participant K).

Further consideration of public awareness of CCTV may reveal the effects of maintaining a camera system that ‘appears’ to prevent crime or at least aid in the apprehension of criminals. In this way, CCTV could actually reduce the incidence of crime by its presence acting as a deterrent rather than its actual effectiveness in crime detection or as an aid to prosecution. This may produce a panoptic effect by maintaining acceptable behaviour in individuals through encouraging the idea that
someone could be watching rather than is watching. This in turn may mean that a lack of public awareness of the shortcomings of such systems may actually aid in its effectiveness.

From another perspective however, the harm to society and individuals that may be wrought over the use of such surveillance may not only be through the undermining of liberties and freedoms. Another concern is the expense of setting up the systems in the first place, and the high level of resources required maintaining the systems. Moreover, there was also concern that CCTV was not so much a supplement to traditional policing but rather, a replacement; there's a lack of police presence now and I sometimes wonder whether it's a trading off... we've got CCTV and we'll concentrate on other avenues (Participant K).

Local authorities bemoan a lack of funds for various projects, and the need for urban development and regeneration, help for the homeless or the elderly to name but a few. It is of concern therefore that the UK government sets priorities to aid in the funding of CCTV; all of a sudden somebody is saying you put 30% we’ll put 70% in for you, you are going to go for it aren’t you? (Participant O). This is particularly worrying in projects that do not actually work properly, are not utilised efficiently at a local level or do not have the manpower resources to operate them effectively; Leicester city centre CCTV operation is now manned by two people running twelve hour shifts each and nobody when they have their day off, and looking at thirty six TV screens each. The council are saying we can’t afford to man it (Participant M).
Although the use of CCTV cameras for surveillance in public places was considered to be acceptable by many participants, they did not accept CCTV surveillance in the workplace as appropriate.

A significant number of Alstec participants were unaware of the level and extent of the monitoring of their email and computer use in the workplace. However, once the computer monitoring was revealed to the Alstec employees, there was little concern about its use, with many staff considering this to be an acceptable restriction on the use of company equipment. This particular lack of awareness could have been resolved by the means employed by H&BBC who decreed that all staff should not only read the use documents, but should sign a form to indicate that they had done so, and understood the limitations and expectations expressed in it.

One chief concern for the participants however was the possible CCTV monitoring of staff. Many of those to whom this proposition was put, expressed a distaste for the kind of monitoring seen as spying, and stated that they would consider this to indicate a lack of trust in the employees. Trust was considered to be a key factor in maintaining a positive working environment. Therefore, any method of monitoring that would undermine this would be greeted with resistance. There was however no indication that those kinds of monitoring tools were either installed or being considered within the two organisations being studied.

5.3.9. Attitudes toward the Media.

In discovering levels of awareness the role of the media was seen as an important issue in many cases. This was not due to the potential for the media to inform and educate,
but rather the problems that may arise due to the media being over zealous in its search
for a story; *I think the media to some extent try to create stories rather than reporting
them at the moment* (Participant G) and the effects that this would have on individual’s
privacy.

One striking revelation from this research was the general distrust of the media,
particularly the popular press, by the majority of participants from both organisations.
When considering perception and awareness of the media, a cynical view was apparent
from many participants who were very aware of the role that the media has to play in
not only the education of the public about issues such as privacy, but also in the
undermining of privacy itself; *they get un-attributed information and leaked stories, its
tjust manipulation. So I think the media is quite a problem in itself* (Participant H).

### 3.10. Age and Position Related Perspectives.

It became clear from very early in the analysis that there were few age motivating
actors amongst individuals where perceptions of privacy were concerned. In some
cases there was some evidence of nostalgia in older participants’ accounts of privacy in
the past. The level of concern and awareness was comparable across the age ranges of
those interviewed. There was some greater level of awareness by some of the more
senior employees and those with longer service records perhaps due to a closer concern
with the organisation and implementation of ICTs.

Here were several participants who were in the older fifty plus age group. These
individuals had spent the early part of their working lives in a paper-based environment,
and had felt the impact of computing technologies more greatly. When asked; *have you
seen computers make a big difference? The older participants were clear as to the huge impact this had had on their working lives. F stated that there had been a tremendous change and G stated; don't do much without one anymore. I suppose it's had quite an effect on me. Whilst there seemed to be little fear of the technology, there was an awareness of the change and concern that use of older manual systems may be seen as old-fashioned. Participant F stated if you're doing something hand written you can think it's silly which indicated a desire to be seen to be up-to-date with technology and perhaps even a fear of being considered out-of-touch.

There was an indication of some initial reluctance, particularly amongst more senior participants to actually use the equipment themselves despite seeing the advantages for the organisation as a whole. However, they had overcome their initial reluctance once the advantages of its use had been fully realised; I needed the communication through email and so on and...instead of asking somebody to do it for me I had to do it myself (Participant H). In general, the older participants had embraced the use of computers and were clear about some of the problems and inefficiencies of the Internet when first starting to use it, as Participant G stated; I think its very frustrating when you start on it, you get better at searching as you go along. This was perhaps highlighted by the lack of training experienced by this participant when he stated that; it was a case of there it is, go play with it sort of thing (Participant G).

It was revealed that there was some reluctance on the part of many of the participants across the ages and positions within the organisations to undertake any form of e-commerce. This was whether through the use of the Internet to make purchases, or online banking. The main reason for this reluctance appeared to be concerns over
security. Furthermore, the older participants had a preference for doing business face to face; *I prefer to go out and pay with money and get mine out of the bank* (Participant K). His was not particularly from the perspective of privacy of personal information; rather, it was due to concerns that their credit card or other financial information may be stolen and abused combined with the maintenance of older traditions and habits.


From the above analysis, several findings were discovered about the impact on perceptions of privacy of the individuals involved in the study. Each of these findings showed perspectives that impacted not only on the daily lives of the participants, but had a considerable effect on the perceptions of privacy within the organisations.

- Many individuals showed a lack of concern at the outset. However, on several occasions participants revealed a higher degree of concern as the interview progressed.

- Many of the participants had a high level of trust in both organisations to protect their private information.

- There was a distinct cultural difference between the public and private sector organisation. There was a more formal and regimented approach to ICT use within the council contrasting with a more open and flexible approach of Alstec. Further, the council was more proactive than Alstec in ensuring privacy protection and compliance with legislation.
• There was an awareness and acceptance of the inevitable loss of privacy if one wished to participate in the benefits of ICT use.

• Many participants had a distrust of the media: although there was an awareness of media influences on the interviewee’s perception of issues.

• Many of the participants found junk mail to be an annoyance but did not see this as an intrusion or privacy invasion but as an inconvenience and waste of time and resources.

• CCTV was not acceptable within the workplace where it would be directly monitoring performance. However, it was seen by many as very acceptable and necessary to prevent crime or to catch criminals.

This section has considered the issues that were revealed most strongly in the interviews. It has analysed the issues by focusing on organisational perspectives and with particular emphasis on answering the two research questions that more directly relate to organisational culture. The principle findings from this analysis and how they relate to the research questions are presented in the concluding chapter of this thesis.

5.5. Interpretive Interactionism and the Analysis of Selected Individuals.

The following section details and analyses the data from the perspectives of the individuals in this study. Although there are some organisational references throughout, these are provided in order to contextualise the data within the lived experiences of the participants. The analysis was conducted by careful consideration of the tools utilised
by interpretive interactionism, which enabled the research questions to be answered by identification of epiphany and its impact on perceptions of privacy. The focus therefore was to discover perceptions of privacy, if the participants believe that privacy is a right, and if they consider privacy to be under threat. Again, the analysis was utilised to further revisit the previous organisationally focused analysis, and contributes to an understanding of privacy perception both organisationally and individually.

This section considers the individuals directly. Two individuals from each organisation were selected, and their interview data subjected to the intense form of analysis necessary to discover their perceptions of privacy.

It was decided that the two selected participants for this stage of the study would include one older and one younger participant. This was because during the initial organisational analysis, it became clear that the sharpest contrasts where they occurred were between the older and younger participants. It should be reiterated here however, that the contrasts were not in the areas of awareness of the issues, or importance of privacy so much as the amount of privacy and the impact of changes in technology. The key issues identified are seen as ‘epiphany’ or ‘life changing’ and provide a starting point for analysis. The further examination of an older and younger participant from each organisation was particularly useful in identifying the different perceptions that the concept of privacy revealed.

Interpretive Interactionism involves a hermeneutic approach to the analysis of an epiphany or ‘life changing event’ in order to discover the hidden or ‘true’ meaning of what was said by a research subject. Hermeneutics involves reading between the lines
of the dialogue, considering the dialectic, the body language, the culture and society
within which the individual resides. This allows the researcher to develop a rapport
with the individual and to put the participant at their ease. In this way, it was
anticipated that the participant would more likely be open and honest in their responses
to questions.

However, the informality of the interview process and the impact of the
researcher/participant relationship may influence the results of the study. Therefore this
has been considered to be both a constraint and an enhancement to the research. The
consideration of the hermeneutic circle of understanding allowed for these influences in
the intuitive process. In this way the perceptions of the individuals concerned become
so familiar through the analytical process that further understanding would only be
possible if further research was to be conducted. Therefore the phenomenon was
considered known within the limitations of the information gathered at the point of
analysis.

5.6. Overview of Individual Perception of Privacy.

The first part of this analysis offers an overview of how individuals felt about privacy
and the growth of ICTs. This particularly relates to personal views and only considered
the organisations as an influence on the perceptions. Organisational perceptions and
how individuals felt that it protects privacy are considered above.

The individuals selected for this study comprised a wide selection of employees from
both organisations, having different demographics, ages, positions within the
organisations and length of service. It immediately became clear during the interviews
and when the transcripts were analysed for themes and impressions, that there was considerable uniformity of views across all spectra. This was the first surprise that the research revealed.

Hermeneutic approaches and interpretive interactive analysis techniques allows that the researcher will bring their own thoughts and preconceived ideas to the research. It enables ideas and expectations to be considered and then changed as the research process continues. In the case of the initial reaction to the questions about privacy by the participants, several assumptions were refuted by the research.

Firstly it was expected that the individuals would be more concerned than they initially indicated, (although in some cases a greater degree of concern was revealed as the interviews progressed). Secondly, it was expected that there would be a noticeable difference in awareness between age groups, considering that older people may not be as aware as their younger colleagues. This however was also found to be untrue. Thirdly it was expected that there would be some differences in the answers to the question ‘is privacy a right?’ Contrary to this, all of the respondents considered privacy to be a right with very few caveats.

These assumptions or biases were brought to the research and rejected during the early stages of the analysis. This enabled the research to consider and reject some ideas during the analysis without the need to continue down a dead end road of enquiry. Rather than attempting to prove or disprove a hypothesis, the intuitive analysis of the interviews was able to consider researcher bias or views as a constituent part of the analysis. This allowed the research to flow and change according to its own
discoveries. Conclusions were therefore drawn from what was revealed by participants rather than based on proving or disproving a theory.

The first consideration was to closely read the transcriptions from both interviews in order to seek out key phrases and statements that related to the participants' perceptions of privacy. It was considered throughout the analysis that the transcription and audiotapes of the interviews was a window into the individuals' interpretation of the questions asked. During analysis the search was for patterns of meaning, statements, assumptions and personal interpretations of the participants own responses. In this way, the analysis was able to gather information and perspectives drawn from the respondents own statements.

The analysis also considered commonalities between the other participants to discover whether perceptions were shared regarding certain attitudes or issues. In order to fully identify individual perceptions of privacy, it was decided that further individual analysis was necessary. Therefore, the following details the process and analysis of four individuals selected for further in depth study.

5.7. Selection Process of Individuals for an In-Depth Examination of Privacy Perception.

The process for selecting participants for greater analytical depth was based in particular on the relationship that developed between the researcher and the participant. Those participants that had the best rapport with the researcher were believed to have delivered a greater degree of openness during the interview. Therefore their data was more comprehensive and detailed in content. The length of the interview was a significant
factor in the selection process, as there was some variation of between twenty and forty
five minutes. This however did not merely reflect the relationship between the
participants and the researcher but also the personality of the participant.

Clearly the more outgoing nature of the participant, the more likely they were to talk at
greater length. Therefore, the length of the interview was not the sole criteria for
selection besides age. Another key factor in selection was how at ease the participants
were during the interview and their rapport with the interviewer. In some cases, the
participants were anxious throughout, others became more relaxed as the interview
progressed, and some appeared to be comfortable with the interview process from the
outset.

Those participants who were anxious and did not significantly relax during the
interview were rejected as possible candidates for further analysis. This was because
the information gathered from them did not contain the in-depth discussion needed to
facilitate intuitive analysis using the above techniques, and often included simple or
brief responses to questioning.

Those who were either relaxed from the outset or became so during the course of the
interview and where the first and second interviews lasted for at least thirty five minutes
were then considered for further analysis. Firstly the original interview tapes were
listened to again. Then the transcribed text of each of the remaining interviews was
read again. This time the intention was not to discover themes or perceptions per se, but
to rediscover the feel and flow of the interview as a whole. From this process the
selection of the final participant for further analysis was decided. This was based on the
free flow of information, thoughts, personal feelings, anecdotes and other indicators of their perception of privacy. Participants were selected who showed little concern with giving a right or wrong or even corporately approved answers. This indicated that what was said was their own and personal opinion.

This section is primarily concerned with the analysis of the perceptions of privacy from an individual's perspective. The analysis systematically went through the steps of Interpretive Interactionism as detailed in Chapter 3. This allowed the identification of an awareness of the epiphany of the individuals, how they felt about the issues, internal debates, and their attitude to privacy both past and future.

5.8. Epiphany

As described in Chapter 3, Denzin (1989) saw locating the epiphany as a starting point for the analysis. An epiphany is an event or series of events in an individual’s life that can be said to have had a transforming impact. A transformational experience may not necessarily be one that is negative, nor may it be a single event, but may be several closely related events that have occurred over time. This may be recognised as transformational once the analytical process has been undertaken.

The use of computers and information and communication technologies in society has been relatively rapid. It can only really be said to have had a major impact on individuals as a whole during the last quarter of the twentieth century. The change however has been considerable, and can be considered transformational particularly within the context of this study.
The analysis below sets out to examine four individuals who have all been impacted by the use of computers both in the workplace and within their personal lives. The analysis of these four individuals highlights the impact that ICTs have had on their perceptions of privacy. This was then placed in the context of life experiences and situation from the participants’ individual and personal perspectives.

The issues discovered during the analysis were considered in each individual case, which enabled further analysis of recurring thoughts, attitudes and opinions of these issues. There was also a close consideration of the participants’ feelings regarding the changes in privacy focus and community that may have impacted on their current perceptions of privacy. This has enabled those perceptions to be better placed into their current context. On completion of this stage, the process of refining the results of the analysis enabled clarification of commonalities, which indicated individual’s perceptions of privacy and the impact of ICTs on those perceptions.

5.9. Alstec Selected Individuals

5.9.1. Participant A

Participant A was selected as the older participant in this in-depth analysis of individual perceptions of privacy in accordance with the above criteria.

5.9.1.1. Epiphany

Participant A had two degrees, the first in mathematics and the second in computing. It was her awareness of the future potential for computers that led to her decision to take her mathematical training into the field of computing. It was clear that the growth in
computing contributed to her making this decision to embrace this technology and become expert in its use. This clearly indicated that ICTs have had a considerable impact on A's life and had contributed to her career motivation and progression. In the case of A, she recognized the potential for the use of ICTs and computing technologies and made a conscious decision to become involved with them from an early point, which indicated the impact of ICTs and computing technologies as being the epiphany or turning point considered in this analysis.

As the main Lotus Notes developer for the company, participant A had a responsible job that involved the ability to access personal email and other documents should this become necessary. Therefore, her perception of the importance of privacy, awareness of the issues and her own views of privacy on a personal basis could be considered as critical in her attitude towards her work.

9.1.2. The Use of Construction Techniques to Discover Themes, which Indicate Participant A's Perceptions of Privacy.

5.9.1.2.1. Interview One

Several issues emerged during the analysis of the first interview with participant A. Firstly, due to her active involvement with computers and ICTs from an early stage in her career, she was acutely aware of the potential for privacy invasion. It could be considered that a heightened awareness of such issues would also engender a high degree of concern. Participant A, due to her awareness of the potential for problems particularly on the Internet was at pains to take steps to ensure some degree of personal privacy. This was evidenced by her use of technical means for protection at her disposal such as the use of a firewall on her home computer. On the whole, participant
considered that privacy was important to her; *I actually rate it quite importantly, if I try something in confidence I expect it to be kept in confidence.* This was particularly noticeable with regards to the distribution of personal information. Participant A further stated that; *people shouldn’t have access to things they shouldn’t.*

Participant A made comments that she was aware of monitoring of Internet and email use within the organisation, but that it caused her little concern. Participant A felt that here she had the use of company equipment during company time, monitoring was legitimate; *I think it’s actually right that it should be monitored.* Her general opinion with regard to the potential for privacy invasion of emails, both at home and at work as that she was not particularly concerned. This was because she felt that most people’s email and personal information was not particularly interesting to anyone and it was unlikely that anyone would bother to look at it. During interview one, participant A showed some concern about protecting her privacy particularly against hackers who could potentially invade her system; *those in the know can actually hack to your pc and can pull the details off your hard drive... that I find worrying.*

Essence, interview one revealed most about her perspectives regarding the company and how well privacy as well as company interests was handled by the organisation. On the whole, she had little concern about organisational behaviour with respect to privacy of personal information. She was at pains to explain that even with her strong computing role within the organisation; she was unable to access personal email and information without specific permission. Therefore, she considered that the company protected personal privacy well.
5.9.1.2.2. Interview Two

Interview two had a more personal focus. Participant A made some statements regarding her thoughts on privacy that conflicted with some statements made during Interview one; *I like my privacy don't get me wrong... but I'm not a particularly private person*. The analysis of this apparent contradiction concludes however, that participant considered that privacy was important generally and she would go to considerable lengths to protect it. Moreover, although she was not obsessive about it she would be concerned about the release of certain private information even if she did not consider the information itself to be of importance. She thereby required permission for the release of such information. Participant A cited an example of going into hospital here some people would keep the reason secret and others would reveal the problem to theirs. Her view here was that the release of information should be the decision of the person involved.

With regard to her protecting others privacy, participant A was quite clear that she could not invade others privacy and would actively avoid doing so; *I would not read their mail... I wouldn't on principle.* This indicated a high level of concern to maintain a oral stance from a personal perspective. A reiterated her caution about sending formation over the Internet and general computer security, with passwords on both her home and work computer.

5.9.1.2.3. Contextualising the Case.

Participant A was selected as one of the older participants, she had considerable computer knowledge, and yet had personal experience of times before computers were
integral in daily life. From an organisational perspective, participant A had only been at
the company for a year prior to the interview. She had been appointed at the time of the
management buy-out and was unable to give an indication of the previous culture within
Istec PLC. Allowing for this however, A's previous personal experiences enabled her
to provide considerable insight into previous attitudes towards privacy from her own
perspective as well as an organisational one.

Then discussing the past and present state of privacy, A considered that society now
have less privacy than in the past not only because of the use of ICTs, but because
society is becoming more open. This she also felt was being engendered into the
population so that previously taboo subjects for discussion have become acceptable to
everyone and not of concern. A was also aware that there were different acceptable
limits to privacy for different individuals and that this could make legislation difficult.

ultimately the most important area of privacy for participant A was that of her own
personal life which was highlighted by the statement; my marriage; I wouldn't discuss
that with anybody. This indicated that although society could be considered to be more
open than in the past, there were still areas of personal life that were expected to remain
private. Although participant A was aware that each individual would have their own
perceptions of the importance of privacy, she also considered that when it came to the
right to privacy; everybody has the same rights to the same amount of privacy. This
statement was particularly related to the privacy invasive techniques used by the press
in order to get a story. Participant A felt that as everyone had the same right to privacy,
and that much media behaviour was inappropriate. This had caused the press to be
viewed in a poor light, a perspective shared by many of the participants in this study.
he use of monitoring and CCTV cameras to observe individuals was considered to be acceptable to participant A provided that it did not encroach into her home or actively watch her whilst working. However, participant A accepted that there would be some reduction in privacy, particularly in public places so that crimes and potential crimes could be either deterred or detected and the perpetrators apprehended. Workplace CCTV monitoring was considered by A to be inappropriate, and she cited a time when cameras had been installed temporarily to dissuade theft in the office. This had made her feel uncomfortable; *it makes you feel self conscious* even though she was aware that the monitoring was not for performance reasons, which she considered unacceptable; *I would not like to be monitored in the office, I think that would be an invasion of my privacy because I would feel as if somebody was watching over me the whole time.*

Then asked about the right to privacy, participant A stated that she felt that this was important. When asked to explain why this was so she had difficulty giving a reason, and indicated that privacy as a right was more a general feeling of how things should be; *I don’t really know, I mean it’s just something I just think we do have a right to. I can’t really explain why I think we have a right to it.* This explanation revealed a feeling that privacy was a right without being able to explain why recurred throughout the interviews with many of the participants expressing similar problems with explanation.

The key themes to emerge from the analysis of participant A’s interviews were

- She was very aware of the potential for invasion of personal privacy and considered that she may be more aware than most.
• She protected her computer from direct threats through the use of a firewall and passwords.

• She stated that she was not a very private person.

• The privacy of her personal life was the main area that A felt was important to protect.

• Everyone is entitled to the same level of privacy regardless of their position in society.

• There is less privacy today than in the past particularly of personal information.

• People are becoming used to and more accepting of privacy loss and society is changing to reflect this.

• Privacy is a right.

• Workplace monitoring for performance is an invasion of privacy.

5.9.1.2.4. Personalising Privacy Perception

Participant A was very aware of the potential for privacy invasion particularly on the Internet and believed that there has been a loss of privacy over the years. She protected her informational privacy well, but did not feel that she was unduly concerned about medical privacy. However she was aware that she had never had an illness that she would consider embarrassing and would therefore feel the need to keep private. The use of CCTV was seen as acceptable for crime prevention and detection but not for
Performance monitoring in the workplace. Participant A believed that privacy was a right and that everyone should have the same amount of privacy regardless of their position in society.

The private sector ethos did not fully become clear until the interviews at H&BBC were analysed. It was only then that subtle differences were highlighted that were more in approach than substance, with less emphasis on legal adherence in any strong form yet compliance being assured through strong business practices. Moreover, participant A had strong moral reasoning for protecting privacy that enabled legal compliance with the Data Protection Act 1998.

5.9.1.2.5. Evaluation

From the above observations, it can be considered that there were two key issues for A privacy and privacy protection. Firstly, financial information that could be abused should be kept private, and secondly, anything that the individual would find embarrassing to be common knowledge should also be protected. The importance of privacy could not be overstated, yet there was also an acceptance that society is less private than it used to be, and that privacy will continue to be eroded. Participant A considered that this would be accepted by society as the ability to access information continued to grow. Privacy was therefore a fundamental right that computers and ICT technologies have the ability to erode. It was considered that it was the responsibility of the individual to ensure that their privacy was protected particularly online and within the home. Participant A was very aware of the potentials that ICTs had brought and had sought to resolve these issues from a personal perspective by immersion and knowledge of the technology.
.9.2. Participant D

Participant D was selected as the younger participant in this in-depth analysis of individual perceptions of privacy in accordance with the above criteria.

.9.2.1. Epiphany

Participant D worked in the payroll department. She was in her late twenties to early thirties and did not have a degree. Participant D initially did not respond well to the interview, but as time went on, her responses became more detailed and open. The life hanging experiences for participant D began to emerge as she described the use of the Internet and in particular the increase in unsolicited mail and telephone calls. This was an area of great privacy concern to her. One of the reasons for this was that she had a velvety year old son who had been subject to unsolicited phone calls from organisations trying to get him to participate in surveys. This was despite his immature voice making obvious that he was a child. As a result of this participant D had begun taking greater steps to prevent such calls than perhaps she would otherwise. In this way, the epiphany or turning point for participant D can be seen as two fold. Firstly, the intrusion into her family life by telemarketers, and secondly the use of the Internet as an integral part of her life, which had become so without really being noticed but which had become embedded within it. The key privacy issue here from D’s perspective was concerned with preventing unwanted intrusion into the home in particular from telemarketers.
5.9.2.2. The Use of Construction Techniques to Discover Themes, which Indicate Participant D’s Perceptions of Privacy.

5.9.2.2.1. Interview One

The initial stages of the first interview with participant D were stilted and highlighted by one-word or simple answers to questions. However, as the interview progressed, participant D became more open and relaxed. There was a lack of concern of the potential for invasion of privacy. She had little awareness of the need for protection of personal information on the Internet, which was sharply contrasted with her desire to prevent junk mail and unsolicited telephone calls. Her low level of concern extended to her lack of awareness as to the contents of the ICT policies sent out to employees; I haven’t obviously read it all, but its like anything, just don’t misuse it.

Then asked about what privacy meant to her however, she was able to give a comprehensive answer that showed a higher degree of awareness than initially indicated; just knowing that the information is secure, where you think it should be, and no-one else can look at it. This was in her opinion regarding bank or pay details, mainly financial, although she also considered personal details should be private. She admitted to actively avoiding commercial use of her information by being ex-directory: home and sometimes seeking out the sources of junk mail and writing to them to ask to be removed from their lists.

was the use of the computer and Internet where her lack of awareness was sharpest. Participant D happily engaged in online banking and e-commerce and had a high degree of trust in the organisations that she did business with. This lack of concern also meant that she had no Anti-Virus or firewall software on her home computer.
Her further lack of awareness as to the potential dangers of privacy invasion was that she appeared to have little knowledge of what she should do if her personal information was abused or intercepted online; If... I was using the Internet and the credit card got sed for something, I would then know where it had come from and I would go to that erson directly. Here she seemed to only consider the physical abuse of her credit cards rather than any virtual danger; I would know if it (credit card) had been used audulently, because I check my statements...I do keep a tight hold on everything so if omething was down I would probably think back to where my bag was.

Whilst participant D felt that she had nothing to hide, she did however see the responsibility of protecting others personal information as a liability, and made certain assumptions that most people do not care too much about their personal information, resuming that it is safe. Participant D also felt that; if you've done nothing then you've thing to worry about, which was a recurrent response throughout many of the interviews.

5.9.2.2.2. Interview Two

Interview two was interesting because participant D had clearly considered some of the issues that had been discussed during interview one and had adjusted her behaviour accordingly. This was particularly evident with her use of the Internet in that she had installed Anti-Virus protection after the first awareness raising interview, and was also considering getting a firewall. She still engaged in e-commerce seeing it as a calculated risk that nothing would go wrong. With regard to junk e-mail or Spam, participant D had decided that the best policy was to just change email addresses when the junk mail came too great. This interview revealed some apparent changes in attitude towards
She considered that its use was legitimate for marketing purposes and to ensure that the most popular goods were on the shelves. However, she also did not participate in prize draws and commercial offers due to the risk of being targeted for commercial mailing; *I don't put my name down for anything because you don't realise that that information is then gonna be passed on.*

With regard to CCTV, participant D had no problems with it in principle and believed that its use in private residential areas was unlikely and not a cause for concern; *I'm not threatened by the fact that it's gonna happen on your doorstep because it won't, they can't cover everything.* As with the other participants, she had no issues with the use of CCTV in public areas and did not see this as an invasion of privacy. One caveat with regard to being surveyed however was that it should be done openly or with permission; *suppose it is do anything you like as long as I agree to it, as long as I know you are doing it with permission.*

Media intrusion into individual’s privacy was an area that was of some concern to participant D whom stated that if she perceived that a newspaper had overstepped the mark then she would discontinue buying it. However, she also considered that, *you give that right up once you become famous* which is in contrast with participant A’s view that everyone should be entitled to the same amount of privacy.

Participant D also felt that it was likely that older people would be less aware of the potential for privacy abuse than younger ones; however, the analysis here has shown that this is not necessarily the case. Many of the younger participants were actually less aware of the issues possibly because they had grown up with the technologies and did
not consider the issues in any depth. The contrasts between participant A and participant D in the analysis show this to be a false assumption made by participant D.

When asked about the way that privacy and its protection had changed, participant D was aware of the changes in society calling it; the disjointed society and considered that people did not know their neighbours as well as in the past. D saw the changes as making people less open from a personal perspective in that the splitting up of communities had lessened one-to-one knowledge. However, with regard to informational privacy, participant D considered that there was less privacy than in the past. This did not bother her unduly though because; *I don't think I am being watched any more than anybody else.*

Workplace monitoring was seen very much in the same light as participant A in that it was fine for security purposes, but if it involved individual performance monitoring it would be unacceptable; *if it was just me they were watching, I wouldn't like that.*

The key observation made by participant D that was not reiterated by any other participant was that privacy was a fashionable subject that would not remain an important issue; *I think it will just fizzle out after a while because it's not interesting anymore...The whole intrusion privacy thing...seems to be a trend of it at the minute.* This is interesting because it appears that although participant D wished to protect her privacy, and she felt it was a right, she had no interest in ensuring that the ability to protect her privacy was maintained.
5.9.2.2.3. Contextualising the Case.

Participant D was selected as one of the younger participants. She had only an end user level of knowledge about the operation of ICTs but used them freely and frequently. He too had been at the company for only one year and was at the same level of company experience as participant A. However, participant D seemed much less interested in the organisational culture than participant A. This may have been because he was a young mother who was mainly concerned with protecting her family from intrusion. She saw her work at Alstec as purely a job to help to support her family rather than a responsibility, which required consideration and high levels of involvement. Her position was at a lower grade than participant A and this may in part explain her lack of interest.

The key themes to emerge from the analysis of participant D’s interviews were

- She was initially unconcerned by the potential for abuse of personal information through the use of ICTs.

- She was more concerned about unsolicited commercial telephone calls and junk mail than loss of privacy of personal information.

- She did not see privacy as an important issue to be protected yet wished to have control over her own right to privacy.

- Workplace monitoring for performance was unacceptable.

- People in the public eye lose their right to privacy.

- If you were doing nothing wrong, there was no need for concern.
• Privacy issues will just fade away and are merely fashionable at this time.

5.9.2.2.4. Personalising Privacy Perception

Participant D was largely ignorant of the real risks to her and her family from privacy invasion. Although she saw a loss of privacy over the years, she stated that this did not concern her. Participant D was more concerned with immediate problems rather than long-term potentials, which was largely due to her strong family focus. Her job involved holding, and taking responsibility for, a large amount of personal information, which she saw as a liability that she would rather not have. There was at no time any consideration of the Data Protection Act 1998 despite her work involving information that would be covered by the Act. However, she did take active steps to protect the information in her care as it was an integral part of her job. This contrasted with participant A and her perception that it was the right thing to do whether it was her responsibility or not.

5.9.2.2.5. Evaluation

Participant D had some very strong views about certain aspects of ICT use, particularly concerning the commercial use of personal information. In this respect, participant D was active in preventing these abuses. However, there was a lack of knowledge and interest in the issues of privacy and its potential for abuse that could create problems for her in the future. What was noticed in particular during the analysis was her dismissal of the discussion of privacy and its protection as being a fashionable subject that would soon be forgotten. This seems to contradict her concerns that she should be asked
permission for the use of her information or to be surveyed. Therefore, it appears that she would rather not think of the issues herself and leave others to consider them, preferably out of the public eye, thus ensuring that her privacy was protected without her having to concern herself about her own protection.

6.10. Hinckley and Bosworth Borough Council Selected Individuals

6.10.1. Participant M

Participant M was selected as the older participant in this in-depth analysis of individual perceptions of privacy in accordance with the above criteria.

6.10.1.1. Epiphany

Participant M was Public Relations Manager for the council. He was in his fifties and had been at the council for eighteen months. His job involved aspects of communications and media work. He offered publicity advice to councillors and was editor and publisher of the Borough Bulletin newsletter and the Borough Guide.

Participant M was very talkative throughout the interview and was very well informed about privacy issues and online security. He had seen great changes in the implementation of computing technologies over the years, and had embraced the technology to a great extent, owning three networked computers at home.

The amount of computing that M participated in showed that ICTs had had a considerable impact on his life and that these factors were clearly transforming ongoing experiences that could be considered an epiphany.
5.10.1.2. The Use of Construction Techniques to Discover Themes, which Indicate Participant M’s Perceptions of Privacy.

5.10.1.2.1. Interview One

Participant M protected his home computers with anti virus software and a firewall. He considered that those who did not protect themselves were stupid not to take personal responsibility. He also took advantage of the fax, mail and telephone preference services to avoid as much un-solicited commercial contact as possible. Like many of participants, M was irritated by the amounts of junk mail, and saw this as a major annoyance that had come about due to the increases in the availability of personal information to commercial organisations.

He used the Internet a great deal, participating in online banking and e-commerce with a high level of trust, whilst checking the privacy protection policies of the organisations he dealt directly with. His role as a magistrate had given him some considerable insight into the use of CCTV for the prevention and detection of crime, and although he considered the concept to be a good one, he had little faith in the quality of the pictures taken. He had never had CCTV evidence brought to him in over ten years as a magistrate. This had led to some concern about its use and the costs of its implementation if it was not actually being used for the purpose for which it was intended. Participant M also had concerns that the quality of the recordings was generally so poor as to render it useless for identification purposes.

The implementation of the Data Protection Act 1998 had created some problems for M during his working day, particularly with regard to sending out the Borough bulletin, which required access to names and addresses. Participant M had strong views that
privacy needed to be protected by the individual as well as through legislation. He was a firm believer in taking personal responsibility.

5.10.1.2.2. Interview Two

Participant M was once again very talkative during the second interview. Participant M felt that the data protection training that he had recently undergone had enhanced his already keen awareness of the issues further. However, his opinion of the Data Protection Act 1998 was that it was both good and bad. Participant M was clearly irritated by what he saw as contradictory or useless legislation. An example given was that; *we are saying that you can't give away information that you can readily obtain on the Internet anyhow.* This was seen by M as an unfortunate state of affairs that would mean that there could be some serious legal loopholes that would allow some operators to get around the Data Protection Act 1998.

Participant M was able to discuss his opinions regarding the changes in the nature of privacy during interview two. His opinion, in keeping with others, observed that there was much less privacy than in the past and that the proliferation of personal information availability was of some concern to him; *it makes you wonder what other information is available if you know how to get it...so much is held on computers.* Participant M felt that there would inevitably be further changes mainly due to the need of politicians to make their mark; *there is always a desire, especially amongst politicians, to change things...because if they don't change things they are seen as doing nothing.* In this way, participant M felt that privacy law would be tinkered with but not hugely changed in the future.
With regard to privacy between individuals, participant M was aware that there was a growing tendency to know less about their neighbours than in the past and yet organisations, both public and private had access to vast amounts of information that was not available prior to the advances in ICTs.

When asked about the concept of privacy as a right, participant M also felt that this was fundamental and yet difficult to pin down in its definition. This was due in part to the differences between individual definitions of privacy; it's very difficult to draw a line about where privacy is because every person will have a different view on it. You have a right to privacy, but that right has to be tempered where your right to privacy affects other people detrimentally.

5.10.1.2.3. Contextualising the Case

Participant M was very aware of the potentials for privacy invasion particularly on the Internet. He was careful to protect his privacy with the use of firewall and anti-virus software and was particularly cautious, whilst participating in e-commerce. He had a high degree of trust in his bank to reimburse him should there be a problem with online fraud and so had no concerns about the use of the Internet for banking and shopping purposes.

The key themes to emerge from the analysis of participant M's interviews were:

- CCTV was useful but lacked sufficient accuracy and clarity in local systems to be effective.
Privacy was a right that should be considered in the light of the effect its loss may have on others.

Individuals should take responsibility for their own protection as far as possible.

The Data Protection Act 1998 has had considerable impact but has also created problems.

Unsolicited mailing, telephone calls etc can be prevented to some extent by the consumer, and were largely an irritation.

Changes to privacy legislation are largely politically driven.

There is considerably less privacy than there was in the past.

5.10.1.2.4. Personal Perspectives of Privacy

Participant M was very aware of privacy issues. He was a strong believer in the individual taking personal responsibility, and saw problems with legislation as being unable to protect personal information properly due to exploitable loopholes. Privacy would continue to be eroded and political changes would directly affect this. Privacy was seen as a fundamental right which needed to be tempered with any potential effects, particularly detrimental, that one may have on others by exercising that right.

Participant M was happy to conduct online transactions, trusting banks and financial institutions to ensure that inappropriate use of credit cards by a third party and so on, was not the responsibility of the consumer. Participant M was aware of the dangers of
information becoming available over the Internet, and therefore protected his computer with a firewall. He admitted however, that if he did not have a knowledgeable friend to install these products and advise of some of the dangers, he may not have had the insight that he currently did.

5.10.1.2.5. Evaluation

Participant M was very knowledgeable, and tried hard to protect both his family and himself from the worst intrusions into his personal life. He was also acutely aware that data protection legislation, whilst a useful tool in preventing inappropriate divulgence of personal information, it could make things difficult from an organisational perspective. His role as a magistrate provided considerable experience of petty criminals, and his surprising revelation that he had never had CCTV used in evidence was disturbing. This was because if it was not being used as a crime prevention/detection tool, then there was a question of what was it was actually being used for, and what was the point of spending huge amounts of money on such systems?

5.10.2. Participant Q

Participant Q was selected as the younger participant in this in-depth analysis of individual perceptions of privacy in accordance with the above criteria.

5.10.2.1. Epiphany

Participant Q, despite being only in his mid twenties was one of the more senior personnel interviewed at the council. He was a barrister who had been working in the capacity of district secretary for one year. His role had a wide remit, involving legal advice to the council on many different issues, and included dealing with various
committees as the need arose. His awareness of the potential for privacy abuse was extremely high, which was due in part to his role of data protection officer for the council. Participant Q was particularly resistant to change in the way that the council conducted its business. Whilst concerned that the council should comply completely with legal requirements, he hoped that it would all go away in the end leaving him to get on with his job.

The epiphany for Q was the strong implementation of the Data Protection Act 1998, which had not yet been fully realized for him. It was considered that Q might find that as there were greater strides towards data protection, national security and the need for joined up government that his workload would increase rather than decrease in coming years. Already, Q had seen severe reactions by staff to the data protection training, which had begun to cause problems of access to information within the council.

5.10.2.2. The Use of Construction Techniques to Discover Themes, which Indicate Participant Q’s Perceptions of Privacy.

5.10.2.2.1. Interview One

Participant Q was very articulate and had some strong views on the subject of privacy. He was also extremely aware of the issues and was able to consider them from both the perspective of his role within the council and from a personal perspective, which did not always concur. From a personal perspective, participant Q was cautious, particularly with regards to financial details. He would not use the Internet for anything that meant that his credit card numbers needed to be sent, which he admitted was creating a few minor difficulties for him when he was trying to book airline tickets and so on.

Participant Q had a high level of trust in the use of CCTV and the organisations that
administer the systems; you rely on trust in those organisations to use the information appropriately...its on trust that they are doing it properly. His knowledge of how the CCTV systems were operated within the council may have led to this level of trust however, he could not be sure that all agencies would operate as ethically.

Commercial use of personal information was not seen as a problem for Q. He did not mind it being used where personal identifiers were lost within the sea of data, but did not like the junk mail that was generated from the targeting of individuals during commercial data collection and sharing. Participant Q considered that his knowledge of the issues was perhaps greater than the majority of the public due to his position within the council, particularly with a view to his wider role as data protection officer.

The changes being made to the way that the electoral register was to be administered was one that participant Q welcomed, although he was unsure if the changes would go far enough to protect people. He tied in his awareness of this change and his knowledge of ways to prevent unsolicited mail to being at the council and conceded that his knowledge would be considerably more limited if he was working elsewhere; I only know about the electoral register and the fax preference service through work...otherwise I wouldn't have a clue.

Participant Q was also aware that his perspectives of privacy protection and the need for greater public awareness of their rights and the issues affecting them did not match well with his role within the council; as a member of the public I would say yes, the media and the organisations involved should tell people when there are changes in the law, or simply tell people what their rights are, as a lawyer I'm all in favour of that. As
somebody who works in the council I can quite do without the press keeping on
drumming home to people what his or her rights are. This shows that participant Q
considered his roles from both personal and professional perspectives and was
comfortably able to differentiate them.

5.10.2.2.2. Interview Two

Interview two had a greater emphasis on personal perspectives than interview one.
However, it became immediately apparent that the Data Protection Act 1998 and its
implementation were having a greater effect than Q had at first envisioned. A
proportion of the interview considered the effects of this on working practices (these
issues are considered in more detail above).

Participant Q was asked about privacy in the past compared to privacy now. He
considered that personal information in particular had become more easily available.
This was to the extent that he would expect that much of his personal information would
be relatively easy to find on the Internet; I would be horrified but I would expect to find
most of my personal information of one sort or another, available over the Internet.

Participant Q did not consider that the use of CCTV infringed on his privacy. This was
because he had become so accustomed to it that he barely noticed it. Also, he had
considerable trust in those operating the systems so that he believed that they were
unlikely to pry into others daily lives; there's not somebody sitting there looking at the
CCTV cameras and thinking oh yes lets find out lots of information.
With regard to the media, participant Q was, like the majority of participants in this study, wary of the press and felt that they have some problems with double standards; the media and privacy don't tend to go particularly close together unless it is their privacy they want to protect. He also felt, unlike participant D, but similar to participant A, that those in the public eye should have as much right to privacy as anyone else. However, he also considered that the public were detached from it and didn't see that the same principles could apply. He also conceded that some people would go out of their way to encourage media attention which meant that they would give up some of their privacy for the privilege of being in the public eye.

Participant Q saw the future of privacy slightly differently from both participant A and D. He felt that the public interest in actually accessing their files would die down. However, this may be a hope on his part due to the increased workload that would be the result of many citizens asking for their details. However, he conceded that the council may actually have a culture shift internally that would protect privacy without having to actually enforce it; we will have shifted and that is probably the biggest impact the acts will have in changing our attitudes. He also indicated that he considered that privacy culturally would continue to be eroded despite the attempts to legally protect it.

When asked about the right to privacy, participant Q considered it to be a limited right. As with many other participants, Q felt that personal privacy in our own homes was the most important right. However, he considered that once we have left our homes and entered into the public realm, we could no longer expect privacy; you automatically interact with other things and people around you. As soon as that happens, there is not...
rivacy. From this perspective, participant Q was aware of the limitations of privacy and where he felt the barriers to intrusion should be set. This was particularly the case where participation in society required certain sacrifices of the right to privacy; as soon as you start being not just an individual but part of society... you offer up some of your privacy.

5.10.2.2.3. Contextualising the Case

Participant Q was a highly articulate and well-educated senior member of staff at the council who is still quite young. He had a well-developed awareness of many of the issues considered here. His acceptance of the public sector ethos within the council was strong despite or perhaps because of his one-year length of service. As he was at the beginning of his career within the council, having been a lawyer and barrister by training, it could be considered that participant Q was still relatively new to the culture within the council. This was initially considered to be why he was operating within very strict parameters. However, this premise was refuted by analysis into the organisation culture shown in the earlier analysis.

Participant Q showed some lack of concern about abuse in some areas, which reflected his experiences within the council culture. An example of this was where he presumed that CCTV was unlikely to be abused, citing personal experience with the way the council operated its system. However, private sector surveillance may not operate under the same kinds of restrictions and consideration of the public interest unlike the public sector surveillance operators.
Participant Q was aware that there were two facets to his thoughts on privacy issues. First were his personal perspectives, which required considerable privacy and protection both within his home, and for his financial information. He was also aware that his strong need for financial privacy and security was leading to some problems with regard to e-commerce and he could envisage future problems in this area. It appeared however that for the foreseeable future, participant Q was not prepared to risk the abuse of his personal financial information for the sake of participation.

Participant Q's second perspective was from an organisational one in that he was aware of the difficulties that strong privacy protection for the public may mean to the council in increased workload and problems with data sharing. In this sense, participant Q openly admitted that from the perspective of being able to operate efficiently, some of the current privacy protections and legislation such as the Freedom of Information Act 2000 and Human Rights Act 1998 made working practices harder and more complex.

The key themes therefore to emerge from the analysis of participant Q's interviews were:

- He was very aware of the issues.
- His knowledge was comprehensive but had some conceptual gaps.
- He protected his personal privacy well.
- Privacy was a 'limited' fundamental right.
- Privacy would continue to be eroded.
To participate in society is to lose some privacy.

- The use of CCTV is acceptable.

### 5.10.2.2.4. Personal Perspectives of Privacy

Participant Q was very aware of the potential for privacy invasion, particularly on the Internet and took steps to protect his information. He believed that privacy of personal information had been considerably eroded over the years and that there was little that could be done about it now. In this respect participant Q believed that it must just be accepted as part of the society we live in. The use of CCTV was considered to be a legitimate way of enhancing crime prevention and he did not perceive there to be any problems with inappropriate operation. Participant Q believed that everyone should have the same right to privacy. However, he also considered that the right is limited to within one's own home, and that once one leaves the home and enters the public sphere, one can no longer expect privacy. With regard to legislation, participant Q felt that although it is possible to alter the internal culture of an organisation in the short term, that eventually if left alone, there would be some drift back into older ways of operation.

### 5.10.2.2.5. Evaluation

From the above observations, it can be considered that participant Q had considerably opposing views regarding privacy, his personal perspectives and his professional perspectives. He appeared to have little difficulty in considering both simultaneously. This may highlight a larger issue in the development and implementation of public policy and privacy legislation in that if the issues were considered from personal
perspectives, then most decision-makers would argue for strong protection and legislation. However, where an organisational perspective is taken, then there are also strong arguments for limiting protection and legislation to enable the efficient delivery of services

5.11. Analysis of Selected Individuals from a Social Psychological Perspective.

Social psychology, as a sub-discipline of psychology provides the tools and language to provide greater insight into the behaviour of individuals (see chapter 2). How the individuals presented themselves to the interviewer, the beliefs stated and the changes in behaviour exhibited as each interview progressed revealed several themes that can be best referred to in social psychological terms. In this way it is possible to highlight further the privacy perceptions of the individuals as an indication of behavioural patterns reinforced by the engagement of the participants with their environment. The increasing awareness of privacy as an important issue reinforces the view that a social psychological analysis of behaviour with a particular focus on the effects of privacy is necessary to enable a greater understanding of individuals within society. Through analysis of the data obtained from the selected participants A, D, M and Q, using a social psychological perspective, four themes emerged that further indicate the privacy perceptions of the individuals studied.

5.11.1. The Presentation of the Self

How an individual presents themselves is an indication of the role that they perceive they have within the world. In this work, each selected individual was interviewed from
two perspectives; as a member of an organisation, and as an individual. From the outset, the participants showed a ‘face’ to the researcher that reinforced the presentation of the organisation. This meant that there was little direct criticism of the organisation’s handling of personal information. I actually think we do quite well there (Participant M), with each individual being concerned to present a view that was positive and in keeping with the tacitly agreed norms and culture of the organisation we are told to be aware, you know, so you don’t just let information float about for anyone to see (Participant D).

In some cases these presumptions were made based on little actual knowledge of the true nature of the protection in place well I’m not really sure how it works, but I don’t know of any major problems (Participant D), but were based on the expectations of the participants that the organisation must have such procedures in place and that they are working effectively even if this could later to be found not to be the case.

The culture within H&BBC was one of outward trust and expectation that everyone would behave appropriately I mean, you don’t get the human resources section leaving their offices open and their files open (Participant Q) but there was also some evidence that a determined individual could probably gain access to information relatively easily and that actual security was not as strong as implied security I know for a fact, there’ll be files open on my desk...or pieces of paper around the room (Participant Q). By giving the outward appearance that information is protected well, it is therefore assumed that it is protected whether or not this is true, leading to a tacit agreement that there is actually strong protection.
The analysis also revealed a difference between the self presented to the world and the self that was kept private. Overall, the individuals were happy to allow many aspects of their lives to be publicly available (see earlier analysis above) and yet other areas were expected to be kept private. These aspects varied according to the particular importance placed on them by the individuals and for various reasons. The most interesting area of protection from a social psychological perspective was the requirement that personal lives such as relationships with family were kept private. I certainly wouldn’t like anyone to see what me and my wife do in the bedroom (Participant M). This personal realm was not however limited to intimate moments between two people. The home itself was identified (with some caveats regarding the apprehension of criminals) as a place where privacy rights should be upheld. This can be seen from the way that it is once one is to leave that domain, one’s rights to privacy become limited by the individual’s interaction with the world. You automatically interact with other things and people around you. As soon as that happens, there is not privacy (Participant Q). Two perspectives can be drawn from this. Firstly, the presentation of the self may be different depending on the social situation and expectations. What is meant here is that if we know are being observed during intimate moments with selected individuals, then it is likely that we would behave differently and that it could prevent or alter the nature of that interaction.

Secondly, this need for a private realm indicates that privacy is important to enable individuals to present their public face only when in the public sphere. The ability to disengage from societal norms and to be oneself is clearly important in enabling the individual to present the social face to the world.
5.11.2. Organisational and Individual Beliefs

Despite the above observations about the differences in the public and private face, it was also evident that many participants did not identify their different and yet overlapping views of privacy within society and privacy within the organisation, seeing their perceptions as being ‘their view’ rather than socially or organisationally constructed.

One participant however, was aware of the differences in emphasis of being an individual and being in an organisation, and was able to self analyse his position. In this case, he was able to hold several different viewpoints simultaneously and to believe in the validity of each depending on the role he was playing at the time. With regard to questions about increasing public awareness of data protection and privacy through the media and education as a member of the public I’m all in favour of that... as somebody who works in the council, I can quite do without the press keeping on drumming home to people what their rights are (Participant Q) his response clearly shows how one can hold conflicting views simultaneously. One, which emphasised the demands for information and fair practices, and the other which sees increases in publicly available information as creating difficulties in the social context of work.

5.11.3. Good or Good Enough?

Another social psychological finding was that the policies of the organisation were believed to be appropriate and ‘good enough’ without the apparent need for too much scrutiny. In some cases, this meant that although the outward presentation of the organisation was one of ethical and secure protection of personal information, there was
awareness that this was not always the case and that occasionally such rules would be
overlooked in order to facilitate the smooth running of the organisation. The behaviour
of the employees within the organisations further reinforced the culture of the
organisation in that where data was accessed, attempts to protect it were seen as a
burden *You know it's a bit of a liability really* (Participant D), but also as an obligation *I
would not read their mail ... I wouldn't on principle* (Participant A). However, there
was also an understanding that on occasion, it may not be practical or possible to
operate precisely within the guidelines set; *I think it's more up to their manager to
uphold that, keep that secrecy between the* (Participant D).

The appearance of information privacy was considered important to be maintained more
than the actual truth of privacy security within the organisation *It wouldn't surprise me
if the information got out by different ways, because the way the system is* (Participant
D) which indicates that security is not as tight as it was indicated to be at the outset.

Social interaction between colleagues may also influence the presentation of the self and
the presentation of the organisation. Individual’s may present themselves differently
depending on the relationship they have with colleagues. In this way, an employee may
present a compliant and contented face to an employer whilst also presenting a less
compliant face to other colleagues. In some cases, such interaction may result in
managers being expected to act to *stop the chat at break times* (Participant D), where
chat could possibly undermine or change the perception of the organisation from the
perspective of its employees or any outsiders who happen to be listening to the conversation.

5.11.4. Articulation of Perception: Interview technique or internal evaluation?

Another theme of interest that was revealed during the analysis was the gradual change of perceptions articulated over the course of the interviews by several of the participants. Initially it could be asserted that many of the views were related without much thought, almost as if they were reproducing perceptions that had been handed to them by the various influencing factors in society and in the workplace. A good example here is the often repeated statement that *if you are doing nothing wrong then it doesn’t matter* (Several participants made similar statements to this across both organisations).

Whilst many of the ideas and perceptions appeared consistent, there were some quite contrasting views that were articulated between what was stated at the outset *I am not particularly bothered about my personal information, I mean its pretty widely available now anyway through the Internet* (Participant D) and what was indicated later *I don’t enter prize draws and stuff, cos I know they pass on my address* (Participant D). This may be due to the participant becoming warmed to the interview process and so becoming more open. However this may also be an indication that the articulation of perception changed over the course of the interview, resulting in the participant identifying the ‘real’ feelings on the issues that were unidentified prior to the interactive process of the interview.
The conclusions to be drawn from this analysis are that the self that is presented to the world where privacy is concerned is greatly affected by the social phenomenon that individuals are involved with. Further, individuals are able to present different ‘selves’ according to the nature of a social interaction. Moreover, individuals will present an organisational image or mask that does not necessarily directly relate to the ‘true’ situation within the organisation, rather they will present an image that is in keeping with the culture and expectations of the organisation in order to maintain their position as a member of that group. In this case, the true levels of security and trust within the organisations was not always (at least initially) indicated by the participants.


Although the information gathered from each of the above individuals was analysed separately, in order for this research to be able to reach conclusions, the analysis must be placed into the context of a much bigger picture. In this case, the individuals have been considered more extensively than the other participants. The individuals’ perceptions of privacy have been highlighted above, with each individual’s opinions being analysed in greater depth, and within their own context rather than a purely organisational one.

This final section has brought together the analysis of the individuals and provides insight into perceptions of privacy from the perspective of those individuals within the study. This is not to say that this evaluation explains all individual perceptions, nor does it lead to generalisation within the population. The evaluation has therefore provided insight into the perceptions of those involved in the in-depth part of the study and
provided some further illumination of the impact of both a public and private sector ethos on individual perceptions of privacy.

The similarities of responses and perception between individuals were initially quite pronounced. This showed a considerable amount of agreement between individuals on some quite fundamental and significant issues. These findings are brought together with the analysis of the organisational perspectives in the final chapter to provide answers to the research questions posed in Chapter 1, and reveal other important perspectives that were discovered during this research.
Chapter 6: FINDINGS AND CONCLUSIONS: A DESCRIPTION OF THE CONTRIBUTIONS AND FUTURE RESEARCH DISCOVERED DURING THIS RESEARCH.

Our life experiences and how we critically reflect on those experiences are important considerations for our personal growth, understanding and development. This study sought to move beyond a reliance on theories formulated by positivistic processes, and into the realm of interpretation in order to explore individual experiences and perceptions of privacy within the organisations studied. In this way, the intention was to explore those perceptions in a more holistic and transformational way than are permitted by positivistic approaches. The hermeneutic approach utilised by this study was appropriate for exploring the meaning of the experiences and perceptions from the point of view of each individual studied, and within the context of his or her own life experience.

The literature reviewed in the study indicated that there appears to be little examination of individuals and the impact that ICTs have had on perceptions of privacy. In particular, the literature did not consider the importance of the lived experiences of individuals and the impact of policies on perceptions. This is a problem because privacy exists within personal relationships and not solely within textbooks. Policy making must thus take into account both theoretical understanding and individual perceptions. This indicates a need for research that addresses this lack by investigating individuals within organisational contexts, whilst also considering their views and opinions from a personal perspective. Further, the literature chiefly focuses on
philosophical, social psychological, legal, organisational or public policy perspectives. Therefore there was a clear gap in knowledge of privacy from a personal or individual perspective.

This research was aimed at filling this gap. The intention however was not to research individuals in isolation, but to draw on previous literature, to inform and ground the research into the context of knowledge already attained. In this way, the study has provided valuable insight into privacy and social psychological perspectives of privacy that had previously been largely overlooked. The use of interpretive interactionism in this context is also a significant contribution. This work shows that using those techniques in this way has not only provided insight into perceptions, but also significantly increased the scope for the technique beyond its original uses as described by Denzin. The findings of this research have therefore increased the body of knowledge in the field of privacy research and qualitative research methods in a notable way.

This work has focused on three areas that impact or has impacted on the perceptions of the participants in this study. Its aims were to consider individual perceptions of privacy and the impact of ICTs on those perceptions from personal, organisational and public/private sector perspectives.

In all, four research questions were identified in Chapter 1. Two questions focus on organisational perspectives;

- **How do individuals within the organisations studied perceive the issues of privacy and privacy protection?**
• What is the relationship between the organisation and the individuals in the study with regard to privacy and policies?

The other questions were more personally oriented;

• Is privacy considered to be a ‘right’ by the participants in the study?

• Is privacy perceived to be under threat with the use of Information and Communication Technologies?

This chapter shows how the findings from the empirical work and analysis have resulted in answering those questions. It will then analyse the research process providing a critique of the work and revealing lessons learned, constraints discovered and the limitations of this research. Finally, future research is considered, identifying issues revealed during this work that would benefit from further investigation.

5.11. Answering the Research Questions

How do individuals within the organisations studied perceive the issues of privacy and privacy protection?

On the whole privacy was considered to be important to the individuals studied, particularly with regard to personal, financial and medical privacy. The key requirement was that individuals should be informed and give consent before information is gathered and used.
The individuals in both organisations were very concerned about the commercial use of personal information and sought to prevent junk mail and unsolicited phone calls. There was also some evidence that organisational and personal views were not always the same with regard to privacy and privacy protection. It was discovered that it was possible to have personal concerns that could have been seen as conflicting with organisational views. However, those individuals who had identified this were able to separate their organisational self from their personal self and thereby operate successfully to uphold the organisational culture whilst maintaining a slightly different stance at a personal level.

The issue of Spam emails was not investigated separately, but the analysis indicated that it was considered in the same context as junk mail by the participants. Many felt that as long as they were law abiding, there was little cause for concern, which showed a high expectation that surveillance and monitoring abilities would not be abused. There was little concern about the civil liberties losses that may occur due to high levels of public surveillance. However, surveillance in the workplace, particularly for performance purposes was very strongly rejected by many of the participants.

There was a high level of awareness of the Data Protection Act 1998 within H&BBC due to the training undergone prior to the study. This had led to some over zealous compliance with the Act to the detriment of some operational processes. Alstec employees however, had little training and were largely ignorant of the Act and its requirements for protection of personal information. However, it should be noted that Alstec did maintain its systems fairly securely with procedures in place to ensure confidentiality of personal information. Therefore only a few minor lapses of security
were identified. Individuals within both organisations felt that privacy was well protected by their employers, although those at Alstec had more concerns overall than those at H&BBC.

**What is the relationship between the organisation and the individuals in the study with regard to privacy and policies?**

There was evidence that the policies were largely developed at management level. This was particularly evident within H&BBC where policies were seen as a little harsh, and senior management decision making considered prescriptive rather than consultative. The top-down approach of H&BBC to management decisions had resulted in frustration in some supervisory staff, who felt that their input was needed to improve efficiency and that their voices were often unheard. There was however a strong public service ethos within the council combined with an active training culture. This meant that H&BBC employees had a very high level of trust in its ability to protect the privacy of employee and public information. Moreover, H&BBC also had very high expectations of its employees to ensure that privacy of personal information was protected. This was shown by its insistence that all staff undertook data protection training to raise awareness of their responsibilities and potential dangers.

The use of the Internet and email within H&BBC was subject to strict controls due to its public purse funding. This was seen by management to require higher standards of scrutiny than those necessary in a private sector organisation. However, this was still considered by some to be too restrictive, which could lead to less efficient use of the facilities in the long term.
Alstec was more consultative in the policy drafting process, with input encouraged from lower level staff, and the final decisions made by management. The policies were seen as fair and reasonable by staff, despite many having not read them completely. This had meant that some employees were unaware of monitoring despite it being clearly laid out in the ‘use’ policies. There was a strong personal responsibility culture within the organisation which meant that individuals were expected to self train, and to largely maintain their own standards within a relatively broad remit. This meant that employees were allowed considerable freedom in the use of ICTs provided that company interests were not compromised. However, the management maintained a supervisory and monitoring role with regard to email and Internet use, thereby protecting the organisation from potential abuses of the system.

The private sector nature of the organisation meant that its chief concerns were those of profitability, efficiency and the maintenance of company secrets. Alstec management considered that a flexible and yet responsible approach to the use of the facilities would promote higher efficiency and a more relaxed working environment for employees. The few minor abuses of the system were not seen as a cause to change their personal use policy.

Attitudes towards privacy were therefore starkly contrasted in the two organisations. Alstec tended to take a liberal and laissez-faire approach whilst H&BBC were very proactive and prescriptive in its approach to privacy protection. This impacted upon the individuals studied who reflected the two approaches from an organisational workplace perspective. However, the levels of general awareness and personal importance of privacy was revealed to be very similar between all participants from each organisation.
From a social psychological perspective, the individuals were keen to present a face to the world that reinforced the culture of the organisation. Although some participants were aware of areas where security could be compromised, the expectation of high security was tacitly agreed by the employees. In this view, the policies and practices within the organisations were viewed by the participants as being ‘good enough’ so that occasional problems were overlooked in the general view of the organisation’s ability to protect personal information.

Is privacy considered to be a ‘right’ by the participants in the study?

Privacy as a concept and right was considered to be very important by all participants. This was a surprise as the expectations were that there would be some diversity of opinion on this. The interviews did however reveal some caveats such as incidents involving crime, terrorism or fraud. However, the most noticeable finding here was that although all participants consider privacy to be a right, there was a difficulty in actually defining or stating why this was the case or in what way. It often involved further discussion during the interview to actually discover the feelings of the participants towards this.

Ultimately, it was discovered that there was one key aspect of privacy that was considered to be a right beyond all others. This was the right to personal privacy. Therefore although privacy of personal information was considered important, this right could be legitimately given up or removed in order to prevent or detect crime. Personal
privacy or that which involves the intimacy between husband and wife, within families or in the home was considered to be a fundamental right. The home therefore was still seen as the focal point to family life and the only forum where it is completely safe to do or say whatever one wishes (within the constraints of the law). In this way, it was discovered that the presentation of the self to the world and the behaviour of individuals will differ according to the social situation and expectations of the individuals. This variation in the presentation of the self was a clear indication of the need felt by the participants to allow the presentation of a public face or a private face and to disengage from expected social patterns of behaviour.

The personal sphere was the only area of privacy that the participants felt should be maintained at all times and which should be considered to be a fundamental right however it was felt by the participants that in cases of child abuse or domestic violence, this could cause the right to privacy to be legitimately withdrawn.

A further finding regarding the right to privacy was that many felt that a person’s position in society should have no bearing on their right to privacy. The greatest concern here was that the media invaded the privacy of people in the public eye beyond “a need to know” or the individual’s desire for self promotion. This had led to invasions of privacy that were deemed inappropriate by participants in this study and had led to a general mistrust in the media’s ability to inform or to be impartial.

Is privacy perceived to be under threat with the use of Information and Communication Technologies?
The introduction of ICTs was perceived to have created a paradigm shift in society's attitudes towards privacy, particularly privacy of personal information. Many of the participants believed that there was considerably less privacy than prior to the introduction of computers. However, the personal privacy mentioned in answer to question three was felt to have increased substantially. This means that privacy was seen to have changed focus. In the past, the participants believed that there had been high levels of information privacy due to its lack of availability. The closer community and family ties at this time also meant that personal privacy was harder to maintain as friends and family often lived in close proximity to each other. Since the introduction of computing technologies, this focus has changed so that information is now widely disseminated and available. However, the perceived loss of community and the increased mobility of the workforce have led to a reduction in the number of personal details that are known by neighbours and extended family. This is because people tend to keep themselves more closed within a small family, home focused unit and not become so involved in the local community.

It was also believed by many of the participants that this is a trend that is likely to continue. The loss of information privacy was not seen to be a major problem provided that permission was sought to use the information gathered. The loss of community and its subsequent lack of personal knowledge by those communities were seen as an ongoing trend and a problem for society as a whole. However, the desire for personal privacy as a right was interesting, as it brought into focus the subjective nature of privacy. The loss of community has led to an increase in personal privacy, thus creating a shift in importance. As privacy of information such as financial or medical details became less important to individuals than in the past, so the privacy of personal life
became more important. Therefore, the threats to privacy were seen as the potential for intrusion into the family or home rather than the use of personal information.

5.12. Considerations for the Organisations Studied.

From the above findings and answers to the research questions, several areas where changes could usefully be made were revealed. There is a need for Alstec to consider privacy and privacy protection more seriously. It appears that there is a need for a greater emphasis on induction and training, particularly for payroll and personnel employees. This will ensure that Alstec employees do not inadvertently allow the privacy of personal information to be undermined and a consequent breach of the Data Protection Act 1998. It would also be desirable for Alstec to ensure that the ICT use policies are read and understood by all employees to counter the possibility of employees inadvertently infringing the policies through ignorance.

Within H&BBC it may be beneficial for there to be a periodical reappraisal of its ICT use policies to ensure optimal use of ICTs. The restrictive approaches to the use of the Internet and email should be considered for revision once the facilities are fully embedded within the council. Further, there should be more consultation with lower level supervisors to ensure that policies not only consider the obligations of the council, but are also workable and recognise the needs of employees and customers at all levels. The perceived culture of trust that was evident from the study should be recognised and drawn on as a strength. The openness and expectations of privacy that was being extended to the customers should also be considered within the organisation so that the
perceived levels of mutual trust could become actual levels of trust. The example of
data matching of council employees is a case in point here.

5.13. Considerations for Policy Makers

The lessons learned from this research have brought into focus some of the needs of
individuals and society with regard to privacy and policies. Therefore, this work
provides significant insight for decision-makers in this arena. By considering
perceptions of privacy at both organisational and individual levels, this work provides a
starting point for policy makers who need to make privacy impacting decisions.

Further, the importance of consultation and consent has been highlighted showing an
effect expectation of involvement and approval prior to policy implementation. Ultimately,
this research has revealed the necessity for privacy issues to be considered at the
beginning of policy development. The importance of privacy should not be overlooked
and although individuals are happy to give up some portion of privacy in order to
participate, this willingness should not be seen as implicit consent. Moreover, privacy
protection should be built in and not bolted on to future decisions.


Although this research achieved the aims set out in Chapter 1, there were some
constraints that meant that the research could have been more conclusive. Firstly, a
larger sample of individuals would have provided more data and therefore may have
revealed different findings. The ability to return to the participants for further
questioning particularly once analysis had begun in earnest would have enabled
clarification of some issues and a greater depth of understanding. The recording
The equipment used during interview was of a low standard resulting in some responses being unclear. Had the researcher been fully aware of those limitations, greater steps prior to the interviews would have been taken to obtain better quality equipment. This, combined with being unable to return for further interviews meant that some perceptions may have been missed or only partially discovered. Given sufficient time, this researcher would have attempted negotiation with the organisations to allow follow up interviews.

The selection of participants at H&BBC was undertaken by the organisation itself and although represented a good selection of employees, was out of the control of the researcher and may have resulted in bias in favour of the organisation. Had the researcher realised the limitations and potential problems of organisational selection, greater steps and negotiation with the organisation would have been undertaken to allow the researcher to make participant selection. However, the participants did not appear to be ‘towing the party line’ or overly positive about the council and therefore this does not appear to have constituted a serious problem for this research.

If the research was to be undertaken again, a three phase interview schedule would have proved helpful, particularly if the final interview was conducted after all of the initial analysis had been completed. In this way, questions could have been asked that were grounded in the original interview findings and could have served to clarify and give more detail to the more fundamental responses to the initial questioning.

Further, a third organisation could have been selected to enable triangulation of comparisons to be made across different sectors. This would have enabled the
organisational influence to be examined in more depth. In this way, organisational culture and the differences in individual perceptions of privacy due to that culture would have been more greatly highlighted. However, time and financial constraints mean that this would have significantly extended the research and analysis process beyond that available at the time of the research.

The use of software packages to collate the data would have been helpful in speeding up the analysis process. This would have been particularly helpful in the discovery of themes and issues across all interviews. The manual process used was very time consuming and may have resulted in missed opportunities for further discovery. The use of transcription packages would also have reduced the amount of time spent getting the interview data into text for analytical purposes. However, the manual transcription process meant that there was a greater familiarity with the nuances of speech than would have been discovered if transcription had been done in other ways.

Further investigation of Local Government initiatives, particularly with regard to e-government would have been helpful to ground the organisational perspectives of H&BBC prior to conducting the interviews as would a more in-depth study of past and future business objectives for Alstec. It would also have been helpful to conduct some of the research within the organisations by spending a period of time observing day to day operations and how privacy was considered from within the working environment.

The innovative and complex nature of the development of Denzin’s Interpretive Interactionism tools for use in this field meant that inevitably there was a degree of
learning by experience. This means that should a second study be undertaken, using the same techniques, more efficient use of time and resources would be possible.

5.15. Recommendations for Future Research.

This research provides a starting point for greater research into individual perceptions of privacy. Several areas of interest were revealed during the research that would benefit from further study. Firstly, the research was conducted during the latter half of 2001. This meant that the second interviews at H&BBC were conducted just after the terrorist attacks on the World Trade Centre and Pentagon in the USA. There was a large amount of interview data gathered that was directly related to the events and whilst conversation around these issues was a useful way of re-establishing rapport at the start of the second interviews, they were not directly relevant to this research. However, further work using this data would be interesting to study the impact of these events on the perceptions of the individuals’ studied in light of privacy perceptions both before and after September 11th 2001. Collaborative research is currently being considered with the Centre for Computing and Social Responsibility at De Montfort University.

Further research that would enhance the knowledge already gained would be to conduct a longitudinal study of individual perceptions of privacy. This could involve a five or ten year analysis of changing privacy perceptions both at individual and organisational levels. The ability to conduct either a longer study of new organisations or to return to the original organisations periodically would provide valuable insight into the development of privacy perceptions. In this way, changes within the organisations could be examined to see the effect of those changes on the perceptions of the
individuals within it. The value of conducting long term studies is that it would enable perceptions of privacy to be evaluated and kept up to date which would further enable policies to be formulated that reflect changing attitudes.

Another valuable area of future research would be to repeat the research using the same techniques to examine different variables. This could consider organisations from within different sectors such as retail, education, financial or medical sectors. This would enable comparisons across a wider range of organisations and would shed greater light on privacy perceptions in organisations. It would also prove enlightening to undertake the study in different countries to enable greater cultural comparisons.

Other techniques for the study of the data already obtained would also shed further light on the findings. If the data was to be analysed using quantitative methods, particularly if further data was to be gained, either from new studies undertaken in different fields as suggested above or by returning to the original organisations, there would be some greater opportunity for generalisation of the findings across a greater area. The techniques used for this research were qualitative and generalisation was not sought in this research. However, statistical analysis would prove useful to discover information from the data that may not have been revealed during the qualitative analysis particularly for the discovery of trends and averages in the results.

Other future research could include asking different questions that would illuminate perceptions in a different way. Questions not asked during this research could be the subject of future enquiry. In this way, a greater body of knowledge could be obtained providing further depth to the initial enquiry. Future research could also attempt to
discover perceptions of privacy using scenarios to gain opinion after reflection. In this way, scenarios could be introduced to the participants prior to interview and their opinions recorded and analysed. This would provide a considered view of perception and would enable the participants to think more deeply thus revealing greater depth. However, it is recognised that in some instances by allowing the participants to think about the issues prior to interview could result in opinions being stated that were more prone to bias or those perceived to the participant to be what the researcher wanted rather than their own thoughts.

Finally, it is recommended that more research is needed in the realm of social psychology with relation to privacy. It is clear from the review of the literature that this area of psychology has largely ignored privacy as an important issue. In view of privacy’s importance and relevance to the way that individuals see themselves and their relationships within organisations and wider society, further social psychological research is needed. This will enable an appreciation of the impact that privacy issues have on individuals perception of the self within society.

5.16. Conclusion

The findings of this thesis provide not only a valuable and practical resource for those researchers wishing to further enquire into individual perceptions, but also provide invaluable insight for those involved in the formulation of privacy policies in whatever field. By utilising the findings of this study, decision-makers would be better placed to understand the impact of their policies on individuals. When new projects and policies
are considered for implementation, the conclusions drawn from this study could be used as a tool to enable a greater degree of awareness of previously unconsidered issues. This may ultimately affect the degree of effectiveness of and acceptance by those affected by those decisions.

No research can sit in isolation. Qualitative social research in particular can not expect to obtain the same results even if the work is repeated within the same environment and with the same participants. Therefore, this work only represents a small albeit significant contribution to understanding of the issues and provides a mere starting point for enquiry. As has been revealed by this research, privacy perception is changing all the time. Future policy at all levels may not adequately reflect need if research is not considered an on-going process. Further research is therefore important to enable decision makers to consider policy that reflects perception within its current context, and which provides insight into the changing perceptions of privacy.
Appendix 1

Key Legislation

Data Protection Act 1998

The Data Protection Act 1998 has been heralded as an improvement to the 1984 Act. The much stronger updated version of this legislation has been designed to offer a greater degree of protection of personal data. They key points of the Act are:

- Personal data shall be processed fairly and lawfully and shall not be processed unless the following conditions are met.

- Personal data shall be obtained for only one or more specified and lawful purposes and shall not be further processed or used beyond that purpose.

- Personal data shall be adequate, relevant and not excessive in relation to purpose for which it was collected.

- Personal data shall be accurate and up-to-date.

- Personal data may only be kept for as long as needed for the purpose collected.
Personal data shall be processed in accordance with the rights of data subjects under the Act.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

Personal data shall not be transferred to a country or territory outside the European Economic Alliance unless they ensure adequate level of protection for the rights and freedoms of the data subjects in relations to the processing of personal data.

There are however some considerations with the implementation of the Data Protection Act 1998. When conducting the research, it was discovered that there were two distinct differences in the organisations where the Act was concerned. Firstly the Private Organisation did not seem too concerned with the Act nor were any of the employees particularly knowledgeable of the details of the Act. When asked about the importance of data protection to them, there was little concern and many considered it to be largely irrelevant to their work. In sharp contrast however, the employees and management of the Public Organisation were very aware of the Act and staff had all undergone training in the implementation and implications of the Act by the time the study was completed. It was also clear that the Public Sector employees had taken compliance with the Act very seriously.

**Freedom of Information Act 2000**

This Act gives general rights of access by individuals to recorded information held by public bodies and those that provide services to them. In doing this it sets out a number
of obligations on public bodies and specifies certain exemptions from the Act. Although not fully implemented to date, the Act must be fully enforced by the end of November 2005 and it is intended that the implementation of access rights will be phased.

Only Public Authorities are covered, for example, central and local government departments, NHS organisations, schools, colleges and universities, police, post offices, etc. Importantly the terms of the Act can be applied retrospectively once a body is bought into the scope of the Act.

There are twenty-three exemptions that exist within the Act and some of these are shared with the 1998 DP Act. Some exemptions exist that apply to whole categories and or classes of information, for example:

- personal information that is covered under the Data Protection Act 1998.
- information relating to investigations and or proceedings undertaken by the Data Protection Act 1998,
- court records, and
- trade secrets.

Other exemptions can be approved if a ‘prejudice test’ shows that the disclosure and would prejudice the interests of the UK abroad or law enforcement. If information is available on the publications scheme then the Public Authority can refuse to provide information in response to a subject access request.

This piece of legislation is relevant only to the Public Organisation studied except where individual rights to access were considered. There was some concern of its
implementation, and also a degree of skepticism by senior management as to the practicalities of its implementation, and whether individuals would actually use it. However, an observation here is not whether individuals would exercise this right to access, all be it with caveats and exemptions, but that the right to access such information exists.


This highly controversial piece of legislation was introduced with very little public information or debate prior to its implementation. The legislation allows that any public authority may obtain comprehensive details of what any person has read watched, and who they have corresponded with, without a ministerial or judicial warrant. The scope of the Act is so broad that it is possible that almost any public authority, police, or other official may access information without difficulty. Although it is expected to maintain data protection under the previous 1998 Data Protection Act, there is little protection given the scope of exemptions that the RIP Act offers.

The Act in brief allows:

- The interception of Internet communications,
- The seizure of encryption keys,
- Access to stored computer data.
- The interception of electronic mail,
The seizure of information on a user's computer;

The seizure of encryption keys.

There is some concern that there are considerable threats to privacy and civil liberties under the Act, but as yet there has been no evidence of its full force being used. The strict penalties for some non-compliance mean that it could be seen as a useful tool for the quietening of dissenting voices or radical politics in the UK.

The penalties include:

- 2 years imprisonment if encryption keys or information is not provided
- 5 years if you reveal that the key has been compromised.

Clearly much of the legislation shown in brief here is unlikely to directly affect the majority of individuals. What is important is that some of it like the Freedom of Information Act 2000 and the Data Protection Act 1998, at least gives the right to individuals to access information on them should they need it and to change any inaccuracies or seek redress. Other legislation such as the Regulation of Investigatory Powers Act 2000 is less clearly beneficial to individuals, although it will no doubt make the detection of criminals and undesirables a little easier for the police and other public authorities. Other legislation such as the Anti-Terrorism Act, have been reactive in nature (this being a reaction to the events of September 11th 2001) that they have failed to be implemented. The reactive nature of legislation as mentioned previously means
that it is often inadequate to address the real issues of concern, or too draconian and therefore fails to be implemented.
References


http://www.alba.org.uk/polls/accuracy.html Accessed 20/03/03


Denzin, N. K. (1989) _Interpretive Interactionism_. Sage: California


Translated by Joel Weinsheimer & Donald G. Marshall


http://www.marxists.org/reference/subject/philosophy/index.htm accessed 07/01/02

Allyn & Bacon: Boston


Santa Clara California 7-10 November 1995


280


Neimietz v Germany, (1992) 16 EHRR 97 http://hudoc.echr.coe.int/Hudoc1doc/HEJUD/sift/472.txt Accessed 02/10/02


Unpublished Phd Thesis. De Montfort University: Leicester


*Business Ethics Quarterly* 8 (4) p.723-724


Roth, I. (1981) *Cognitive Psychology – perception (part 1)* The Open University Pres:
Milton Keynes


286


Wakefield, J. (2000) Orange sacks forty over Internet porn. ZDNet UK
http://news.zdnet.co.uk/story/0,s2081158,00.html


http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.htm Accessed 13/12/01


Bibliography


Epic, (1999) “Privacy centre calls for strong protection for users” - EPIC says current policy will erode online privacy. www.EPIC.org


www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html Accessed 09 05 00

Cities in a global society, conference paper, Technologies for e-government and

http://www.ed.uiuc.edu/EPS/PES-Yearbook/95_docs/haig.html Accessed
28/02/02

Technology on Privacy in the Workplace. Business and Society Review 102
(103) p. 1-24

http://idpm.man.ac.uk/wp/igov/index.htm Accessed 03/03/03

http://www.man.ac.uk/idpm/idpm_dp.htm#ig Accessed 03/03/03

Blackwell: Oxford

Hirji, K.K. (2001) Exploring Data Mining Implementation: How large volumes of
Organisational data can be exploited for sustained competitive advantage.
Communications of the ACM. July 2001 44 (7) p.87-93

Hodgins, R. (2002) Privacy Trends: Complying with New Demands Treasury Board of
Canada Secretariat. (presentation)


http://www.sociology.org/content/vol03.004/mcgettigan.html

Accessed 21/10/03 Blackwell: Cambridge MA


Mill, J.S. (1884) *A system of Logic*.


accessed 10/06/02


National Institute of Mental Health *Perception, Attention, Learning and Memory* http://www.nimh.nih.gov/publicat/baschap3.cfm#sensat Accessed 15/01/02


http://www.gla.ac.uk/departments/sociology/Compliance2.pdf Accessed 20/06/02


http://www.concord.org/intl/cbe/pdf/thomas.pdf Accessed 05/06/02


UDHR (Universal Declaration of Human Rights) (1994) Article 12
http://www.hrweb.org/legal/udhr.html Accessed 07/10/02


