PhD Thesis

The role of Information Systems professionals in the provision for privacy and data protection within organisations, systems and the systems development process

Richard Graham Howley
Research Associate
Centre for Computing and Social Responsibility
De Montfort University Leicester UK

Submitted in partial fulfilment of the requirements for the

De Montfort University

Degree of Doctor of Philosophy

October 2007
Abstract

The knowledge gap that this research addresses concerns the role of Information Systems (IS) personnel in the provision for privacy and data protection (PDP). The starting point for this research concerns several related theoretical propositions. These include:

1. IS personnel are increasingly involved in the provision for PDP.
2. The precise nature of that involvement is not defined.
3. It is unclear whether members of the IS profession are aware of this responsibility and whether they are equipped to meet it.

This is the knowledge gap this research addresses.

The literature review confirms the involvement of IS personnel but does not provide insights into what form that contribution can actually take. The literature focuses on high-level aspirational descriptors, such as, ‘design for compliance’ and ‘apply privacy enabling technologies’. It is also suggested that there is a low level of awareness regarding PDP issues within organisations. The literature review concludes by proposing research that seeks to discover levels of PDP awareness amongst IS personnel and insights into how they feel that PDP can and is being provided for within UK organisations.

A review of research approaches and methods followed which concluded by proposing that a questionnaire survey would be undertaken into levels of awareness and PDP practices and that this would be followed by an in-depth case study of three organisations.

Analysis of the survey data shows that IS personnel are significant in the provision for PDP and that this is accepted as a legitimate part of their role. The survey shows which staff are regarded as having the greatest contribution to make and at what stage of a development lifecycle that contribution can be made.

Case study research was then undertaken within three organisations seeking detailed insights into how these organisations have responded to the challenges of PDP on their IS and DP personnel and practices. Within the case studies IS personnel were far
less accepting of a PDP responsibility than the survey data suggests. Data was seen as the property of the client and so was the PDP responsibility. Case study respondents were able to suggest the IS staff and development practices that they felt offered the greatest potential for PDP leverage. Amongst the IS case study respondents PDP is seen as largely a security issue and it is felt that this may limit their contribution.

This research and thesis documents the role of IS personnel in the provision for PDP for the first time.
Acknowledgements

This research, and its resulting thesis, was completed over an extended period of time during which life inevitably presents a range of challenges that one has to overcome. The encouragement and support of a number of key individuals have enabled this research and thesis to be completed despite the personal and professional challenges that have sought to deflect attention away from the research.

It is with a huge amount of appreciation that I wish to acknowledge the contribution of the following individuals:

**My wife Marie and my children Rosie and Oliver:** Without the support of my wife this work would never have been completed. She has made 'space' for me, she has created time for me and she has encouraged me throughout this research. Rosie and Oliver have never known life without PhD work needing to be done and I am grateful for their acceptance, at too young an age really, of my need to work and not to play with them on too many occasions. This was especially true during the period when the thesis was nearing completion.

**Prof. Simon Rogerson:** It was Simon’s commitment to research, his welcoming academic style and his commitment to socially responsible computing that encourage me to explore with him some fledgling research ideas that I had been developing over a number of years. During the process of supervision he always encouraged me, supported me and provided both praise and criticism as the circumstances dictated. Without Simon’s support, encouragement and tolerance this work would have fallen by the wayside years ago.

**Dr. N.B Fairweather:** Ben has supported this research from the very beginning and has been instrumental in bringing it to fruition. At every step of the way Ben has been a huge support and never once complained at my late delivery of documents to review or the other, often unreasonable, demands I have made of him. He has always managed to find time to review materials with an impressive degree of precision and insightfulness; for this I will always be grateful. Leading, by example, Ben encouraged me to critically evaluate not only the content of my work but the words
that I use to describe it. This is one of the many skills that I will try and develop further as a consequence of my association with Ben. I am truly appreciative of Ben’s support, encouragement and the huge amount of work he has invested my research, the thesis production and my ongoing professional skills development.

Prof. Lawrence Pratchett: Lawrence played an important part in the early research and in particular in supporting my considerations of policy networks and local authorities. Just as important as that, however, was the encouragement he extended to me during those early years and I never forgot that encouragement in the tough years that followed. Again, I appreciated his involvement and support for this research.

School of Computing: I wish to formally state my appreciation to the Head of School of Computing, Peter Messer, for his support throughout this research. Peter and the School provided financial, professional and personal support during the research and I am grateful for that.

Richard Howley
October 2007
Table of contents

Abstract ii
Acknowledgements iv
Table of contents vi
List of appendices ix
List of tables x
Abbreviations and conventions xi

Chapter 1: Introduction

1.1 Introduction 1
1.2 Research rationale and the knowledge gap 2
1.3 Research Aims 3
1.4 Structure of the thesis 4

Chapter 2: Literature review

2.1 Rise of the privacy and data protection legislative framework 7
2.2 IS personnel, privacy and data protection 18
2.3 Is the environment conducive to IS personnel contributing to privacy and data protection? 22
   2.3.1 Awareness 22
   2.3.2 Commitment 27
   2.3.3 Policy Networks 38
   2.3.4 Role of the Information Commissioner 43
   2.3.5 Other explanations that may inform levels of awareness 45
2.4 Review of research aims and questions following the literature review 47
2.5 Proposed research resulting from literature review 48
2.6 Literature review conclusions 49

Chapter 3: Research Approach and Methods

3.1 The quantitative and qualitative distinction in IS research 51
   3.1.1 Quantitative research 51
   3.1.2 Qualitative research 52
3.2 The underlying epistemology of qualitative IS research 54
   3.2.1 Positivism 54
   3.2.2 Interpretive 55
   3.2.3 Critical theory 57
3.3 Research Methods 58
   3.3.1 Action research 58
   3.3.2 Case study 59
3.4 Data gathering techniques 69
   3.4.1 Interviews 69
   3.4.2 Questionnaires 71
   3.4.3 Observation 74
3.5 Proposed research approach and method 76
3.6 Data Analysis Strategy
3.6.1 Grounded Theory
3.6.2 Data analysis of questionnaire data
3.6.3 Data analysis of case study data
3.6.4 Suggested data analysis approach
3.7 Conclusion on approaches and methods
3.8 Testing the research questions: Two scoping studies
3.8.1 Scoping study 1 - Levels of awareness
3.8.2 Data Analysis: Scoping study 1 – Levels of awareness
3.8.3 Scoping study 2 - Role of IS personnel
3.8.3.1 Data Analysis: Scoping study 2a - Which IS personnel and which principles?
3.8.3.2 Data Analysis: Scoping study 2b - The nature of the relationship between IS personnel and the DP principles
3.9 Scoping studies, research questions and the relationship to further research

Chapter 4: Survey – Levels of Awareness and IS personnel in the provision for PDP
4.1 Research Questions and methodological issues
4.2 Questionnaire design
4.3 Sampling
4.4 Questionnaire results and data analysis
4.4.1 Which IS personnel and what activities present PDP enhancing opportunities?
4.4.2 Are IS personnel equipped to meet the challenge?
4.5 Contribution to theory and refining research questions

Chapter 5: Case Study - Role of DP and IS personnel in the provision for PDP
5.1 Research questions and methodological issues
5.2 Preparation for the case study research
5.2.1 Finding cases
5.2.2 Piloting research instruments
5.3 Data analysis strategy and procedures
5.4 Case study description and justification
5.5 Case study: Analysis and findings
5.5.1 Role and background of respondents
5.5.2 Management of DP
5.5.3 Evaluation of effectiveness of PDP
5.5.4 Improvement strategies
5.5.5 Information Systems Development
5.5.5.1 Whether PDP is a legitimate concern of IS personnel
5.5.5.2 Stages in the ISD life cycle in which IS can make significant contribution
5.5.5.3 What contribution can IS personnel make to PDP?
Chapter 6: Analysis and synthesis: Survey and case study findings
6.1 Data analysis strategy revisited 151
6.2 Findings: Research questions, objectives and theoretical propositions
   6.2.1 Question 1: What is the role of IS personnel in the provision for PDP within systems and organisations and how aware and accepting are they of their obligations? 152
   6.2.2 Question 2: What aspects of IS professional practice have PDP enhancing opportunities and how widely known or applied are these? 154
   6.2.3 Question 3: What is the role of IS management in the provision for PDP and how does that interface with other DP managers in organisations? 154
   6.2.4 Findings in relation to the research objectives 155
   6.2.5 Findings in relation to the theoretical propositions 158

Chapter 7: Conclusion, review and critical evaluation
7.1 Research aim, questions and original contribution 160
7.2 Evaluation of the research process 161
   7.2.1 Methodological context 161
   7.2.2 Data analysis aspects 163
7.3 Evaluation of the research findings 163
7.4 Research achievements 164
7.5 Significance and limitations of the findings 165
7.6 Further research in this field 166
7.7 Concluding remarks 166

References 167
<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>De Montfort University - Ethics form for survey research</td>
<td>176</td>
</tr>
<tr>
<td>2</td>
<td>De Montfort University - Ethics form for case study research</td>
<td>179</td>
</tr>
<tr>
<td>3</td>
<td>Case study consent form for participants to read and sign</td>
<td>181</td>
</tr>
<tr>
<td>4</td>
<td>Case Study Protocol (including interview questions)</td>
<td>185</td>
</tr>
<tr>
<td>5</td>
<td>Survey Questionnaire: ‘Survey of Information Systems Professionals’ role in the provision for Privacy and Data Protection’</td>
<td>199</td>
</tr>
<tr>
<td>6</td>
<td>Covering letter to accompany the postal survey</td>
<td>205</td>
</tr>
<tr>
<td>7</td>
<td>Covering email to accompany the web based survey</td>
<td>206</td>
</tr>
<tr>
<td>8</td>
<td>Survey data showing responses as percentages</td>
<td>207</td>
</tr>
<tr>
<td>9</td>
<td>Summary of the survey data</td>
<td>216</td>
</tr>
<tr>
<td>10</td>
<td>Criteria for selecting industry sector for inclusion in the case study research</td>
<td>226</td>
</tr>
<tr>
<td>11</td>
<td>Letter sent to potential case study organisations</td>
<td>227</td>
</tr>
<tr>
<td>12</td>
<td>‘Frequently Asked Questions (FAQs)’ document sent to potential case study organisations</td>
<td>228</td>
</tr>
<tr>
<td>14</td>
<td>Conference paper presented at ETHICOMP 2004: University of the Aegean April 2004</td>
<td>242</td>
</tr>
<tr>
<td>16</td>
<td>Institute of Management Information Systems Journal article “IS staff and the provision for privacy and data protection” December 2002</td>
<td>261</td>
</tr>
</tbody>
</table>
## List of tables

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Table number</th>
<th>Table title</th>
<th>Page number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2</td>
<td>2.1</td>
<td>Awareness of data users obligations 1999-2000</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>2.2</td>
<td>Awareness of data protection rights 2002-2006</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td>Concerns regarding how organisations use personal information</td>
<td>25</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>3.1</td>
<td>Four types of generalisations from interpretive case studies</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>3.2</td>
<td>Principles for conducting information systems field studies</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>3.3</td>
<td>Eight evaluative questions to determine the suitability of the interview method</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>3.4</td>
<td>Eight steps to questionnaire design</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>3.5</td>
<td>Seven steps to grounded theory</td>
<td>79</td>
</tr>
<tr>
<td></td>
<td>3.6</td>
<td>Guidelines for processing questionnaire responses</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>3.7</td>
<td>Case study data analysis techniques</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>3.8</td>
<td>Scoping study 1: Questionnaire responses</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>3.9</td>
<td>Scoping study 2a: IS roles that can contribute to DP principles</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>3.10</td>
<td>Scoping study 2b: DP principles supported by IS staff</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>3.11</td>
<td>IS Roles with generic associations with data protection principles</td>
<td>98</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>4.1</td>
<td>Economic sector and respondent analysis</td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>4.2</td>
<td>IS roles in the provision for PDP</td>
<td>106</td>
</tr>
<tr>
<td></td>
<td>4.3</td>
<td>Stages in the systems development lifecycle offer opportunities for PDP enhancements</td>
<td>107</td>
</tr>
<tr>
<td></td>
<td>4.4</td>
<td>Awareness of PDP policies</td>
<td>110</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>5.1</td>
<td>Stages in the development of data analysis codes</td>
<td>125-6</td>
</tr>
<tr>
<td></td>
<td>5.2</td>
<td>Data analysis categories resulting from initial data analysis</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>5.3</td>
<td>Occupational roles for data analysis</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>5.4</td>
<td>IS personnel with the greatest contribution to make</td>
<td>143</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>6.1</td>
<td>Research findings in relation to the research objectives</td>
<td>155-7</td>
</tr>
<tr>
<td></td>
<td>6.2</td>
<td>Research findings in relation to the theoretical propositions</td>
<td>158-9</td>
</tr>
</tbody>
</table>
## Abbreviations and conventions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>BA</td>
<td>Business Analyst</td>
</tr>
<tr>
<td>BCS</td>
<td>British Computer Society</td>
</tr>
<tr>
<td>CBI</td>
<td>Confederation of British Industry</td>
</tr>
<tr>
<td>D</td>
<td>Developer</td>
</tr>
<tr>
<td>DP</td>
<td>Date Protection</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>DPR</td>
<td>Data Protection Registrar</td>
</tr>
<tr>
<td>DS</td>
<td>Data Sharing</td>
</tr>
<tr>
<td>DTL</td>
<td>Development Team Leader</td>
</tr>
<tr>
<td>EC</td>
<td>European Community</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FCO</td>
<td>Foreign and Commonwealth Office</td>
</tr>
<tr>
<td>FOI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>HMSO</td>
<td>Her Majesty’s Stationary Office</td>
</tr>
<tr>
<td>IC</td>
<td>Information Commissioner</td>
</tr>
<tr>
<td>ICT</td>
<td>Information Communication Technologies</td>
</tr>
<tr>
<td>IMIS</td>
<td>Institute of Management Information Systems</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>ISD</td>
<td>Information Systems Development</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITM</td>
<td>Information Technology Manager</td>
</tr>
<tr>
<td>LA</td>
<td>Local Authority</td>
</tr>
<tr>
<td>NHS</td>
<td>National Health Service</td>
</tr>
<tr>
<td>ODPR</td>
<td>Office of the Data Protection Registrar</td>
</tr>
<tr>
<td>OIC</td>
<td>Office of the Information Commissioner</td>
</tr>
<tr>
<td>PA</td>
<td>Public Authority</td>
</tr>
<tr>
<td>PDP</td>
<td>Privacy and Data Protection</td>
</tr>
<tr>
<td>PET</td>
<td>Privacy Enhancing Technology</td>
</tr>
<tr>
<td>PN</td>
<td>Policy Network</td>
</tr>
<tr>
<td>PPP</td>
<td>Public Private Partnership</td>
</tr>
<tr>
<td>SA</td>
<td>Systems Analysis</td>
</tr>
<tr>
<td>SD</td>
<td>Systems Development</td>
</tr>
<tr>
<td>SDLIC</td>
<td>Systems Development Life Cycle</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>WSIS</td>
<td>World Summit on the Information Society</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

1.1. Introduction

This research focuses on the role of Information Systems (IS) personnel in the provision for privacy and data protection (PDP). Since the early 1970's PDP has become acknowledged as a major concern of governments leading to a 'growing trend towards the enactment of comprehensive Privacy and Data Protection Acts around the world' (EPIC, 1999). Bloor (2003) points out that legislators across the world are 'enacting tougher privacy and data protection legislation'. More recently, Data Protection and Privacy Commissioners from around the world agreed to 'promote the recognition of the international character of data protection principles .... [and] .... for the development of a universal convention for the protection of individuals with regard to the processing of personal data' (ICDPPC, 2005). This request was then presented to the World Summit for the Information Society (WSIS) that met in Tunis in November 2005. The Chairman of the International Working Group on Data Protection in Telecommunications advises the WSIS that 'Data Protection and privacy are human rights in a global information society and should be taken into account in any new setup for internet governance' (Dix, 2005). We are witnessing a huge expansion in the global provision for PDP accompanied by the increasing involvement of a wide range of new participants including IS personnel. The responsibility to deliver data protection and privacy is being firmly directed at the IS profession and this research investigates the extent to which the profession is willing and/or equipped to respond to this responsibility.

Data protection (DP) provision in the UK is a direct consequence of European Community (EC) membership which now plays a fundamental role in initiating legislation that is then implemented in all European member states. A consequence of this is that EC member states now have a DP regime that is regarded as a model for the world to follow (Ross, 2001). However, despite the current role of the EC, the origins of a national DP system in the United Kingdom (UK) can be traced back to the Younger Committee of 1972 (HMSO, 1972) and the Lindop Report, published in 1978 (HMSO, 1978), which gave rise to the 1984 Data Protection Act. More recently we have
witnessed the passing of the 1998 Data Protection Act, the Freedom of Information Act 2000 and a range of PDP regulations governing the use of personal data in marketing.

1.2 Research rationale and the knowledge gap

Whilst there is a growing body of literature (Raab, 1999; ODPR, 2000; Watts and Macaulay, 2002; Lederman et al, 2003) that promotes the role of IS personnel in the provision of PDP, there is none that provides ‘life-cycle’ coverage of the opportunities to contribute. The literature review (see section 2.2, p18) does identify areas in which IS personnel can contribute to PDP, for example, through the use of anonymising data using ‘personal identifiers’ (Hes and Borking, 1998). Others have emphasised the need to consider PDP in the design of E-Commerce security (Anton and Earp, 2000). Lederman (2003) highlights the relationship between DP and data quality whilst Watts and Macaulay (2002) provide guidelines on how to embed PDP through systems design. At present there is a growing body of ‘aspirational’ literature that promotes the contribution of the IS profession in the provision for PDP but, as chapter two shows, no literature was found that assesses the willingness of the profession to accept this responsibility, or what their precise contribution is, or can be, and how they can deliver it. Underpinning concepts such as ‘willingness’ and ‘contribution’ is the issue of PDP awareness; this research found no evidence that levels of PDP awareness amongst IS personnel had been investigated and reported. Clearly, a willingness to contribute alone is insufficient if that willingness is not built upon an awareness of the legal requirements for PDP and the professional practices that can be employed by IS personnel to contribute to compliance. ‘Awareness’, ‘willingness to contribute’ and ‘how to contribute’ are the knowledge gaps that this research addresses and in doing so it presents new empirical and qualitative insights into how IS personnel can and do contribute to the provision of PDP. It also identifies a range of strategies that are being used to support the development of PDP-sensitive systems. In doing this, the research positively advances knowledge in this area and fills the identified knowledge gap.
1.3 Research Aims

This thesis reports on an investigation into the role of IS personnel in the provision for PDP at both information systems and organisational levels. In addressing these issues the research draws upon developments taking place on a global scale with regard to the PDP and, crucially, the responses of IS personnel. It then contextualises those developments within the European legislative framework and finally provides insights into how a small number of UK based organisations are responding to these developments. The research identifies both perceived and actual roles that IS personnel have with regard to PDP and in doing this the research is guided by two initial research questions:

1. What is the role of IS personnel in the provision for PDP within systems and organisations and how aware and accepting are they of their obligations?
2. What aspects of IS professional practice have PDP enhancing opportunities and how widely known or applied are these?

In addressing these research questions the objectives of this research are:

1. Establish actual levels of PDP awareness amongst IS personnel within a small number of UK based organisations.
2. Identify and explore the attitudes and perceptions IS personnel have with regard to their role in the provision of PDP and assess the impact these have on the IS development process.
3. Identify the extent to which IS personnel are aware of their legal responsibilities to use privacy enhancing technologies and strategies.
4. Identify which stages and practices within the systems development process IS personnel feel they have a PDP contribution to make.
5. Explore the relationship between Data Protection Officers (DPOs) and IS personnel in the provision for and management of PDP.
6. Improve the provision for PDP by enabling the wider distribution of examples of good PDP practice in organisations and the systems development process.

A third research question is added and discussed on page 114.
7. Encourage IS personnel to consider their role and professional practices in relation to PDP.

1.4 Structure of the thesis

Chapter two provides details of the literature review that was undertaken to explore the role of IS personnel in the provision for PDP. The review sought confirmation that IS personnel are being assigned specific responsibilities for contributing to PDP and sought evidence of their ability and willingness to respond to this challenge. Issues such as awareness of PDP, commitment to PDP and the role of the Information Commissioner (IC) are examined to further understand the role of IS personnel in the provision for PDP. Literature is presented confirming the increasing contribution that IS personnel are expected to make. However, little evidence was found that supports the view that they are, as a profession, equipped to contribute effectively at this time. The literature review found that within organisations, awareness of PDP obligations is at a low level which may justify a questioning of how well data is protected in systems and organisations. The literature review seeks explanations for the reported low levels of awareness found, and in doing so it focuses on the involvement of IS personnel and the wider data processing community in the creation of PDP legislation, the formal organisation of the IS profession, their formal and informal patterns of interaction and the role of the Office of the Information Commissioner (OIC) in promoting awareness of PDP. It is shown that none of these explanations adequately explain the reported levels of PDP awareness. The literature review concludes with two related and significant findings. Firstly, during the period leading up to the enactment of the 1998 Data Protection Act (DPA) and during subsequent years many organisations were unaware of their obligations to data subjects, and secondly, IS personnel are increasingly identified as having a key and unique contribution to make in the provision for PDP. The chapter concludes that no adequate explanations exist for current levels of PDP awareness and that further research is required to:

1. Establish empirically levels of PDP awareness and commitment amongst IS personnel.
2. Identify and document the contribution that IS personnel and their managers can make to the provision for PDP.
Chapter three considers the methodological issues that need addressing before the research questions are addressed further. It starts with a review of the major research approaches that are used in IS research and explores the relationship between approach and method. A review is then undertaken of the major methods that are used in IS research leading to a proposed research approach and set of associated methods for use in this research. Data analysis strategies are then considered and a proposed strategy for the actual analysis of the data that will be generated in this research is proposed and justified. The selected methods, research instrument and data analysis strategy are then tested in two scoping studies, the outcomes of which are reported in the concluding sections of this chapter. These studies provide tentative evidence that levels of PDP awareness amongst IS personnel are indeed low whilst the recognition that they have a contribution to make is high. They also confirm that the profession does have a contribution to make and the research instrument used in the second of these studies is capable of identifying particular contributions that can be made in the provision for PDP. The outcomes of these studies confirm the knowledge gap and support the subsequent research that builds on and further develops the findings of both the literature review and the scoping studies.

Chapter four reports the outcome of a survey undertaken to establish empirically how aware IS personnel are regarding their PDP responsibly, how committed they are to contributing to PDP and insights into how they feel they can contribute. The chapter outlines a range of methodological issues that were considered as part of the survey design and presents the conclusions that were drawn from the data analysis. The conclusions are then used to inform a review of the research questions and to feed into subsequent research.

Chapter five reports on the case study research that was undertaken to provide more detailed and qualitative insights into the role of IS personnel in providing for PDP than that provided by the survey research. The chapter outlines the methodological considerations that gave rise to the selection of the case study method being used to investigate the role of IS personnel and their management in the provision for PDP. The relevant research design, data analysis strategy, implementation issues and the findings of the case study research are all reported in this chapter.
Chapter six aggregates the findings of the literature review, survey and case study research, considering them in terms of their overall contribution to the research questions and objectives and shows how this research fills the knowledge gap identified in section 1.2.

Chapter seven concludes the thesis by evaluating the research methods, procedures, findings and achievements. The chapter ends by proposing further research that builds on the research reported in this thesis.
Chapter 2: Literature review

Having suggested that IS personnel have a key contribution to make in the provision for PDP it has been further suggested that they are not equipped with the knowledge or skills to contribute effectively. In order to assess the validity of these suggestions a review of the available literature was undertaken and it is the findings of that review to which we now turn. Before looking at the research questions that constitute the core of this research it is first necessary to review the provision for PDP that currently exists in the UK and the processes that were involved in bringing it about. In examining the framework and the processes involved in its creation it will be possible to suggest answers to the research questions and objectives identified in section 1.3.

2.1 Rise of the privacy and data protection legislative framework

The provision for PDP that exists in the UK is the result of several decades of legislation. This legislation provides a thorough and comprehensive framework that can be used to illustrate our societal response to the requirements to protect privacy and personal data. Before examining the actual legislation it is worth highlighting some possible outcomes of this process. During recent decades we have been subjected to two major DPAs, 1984 and 1998, a Freedom of Information Act 2000 and a whole range of further Acts, regulations and secondary legislation concerning PDP. A consequence of this is that the legislative environment is particularly complex; Acts are closely related to each other, they replace and/or update each other, they are subject to changes and amendments that emerge from secondary legislation and/or the dynamics of ‘bargaining’ during the implementation process (Gerston, 1997, p111). Anomalous situations have arisen in which PDP Acts contradict each other leading to a situation in which compliance with one Act may constitute an infringement of another. The section that follows outlines the features of the main PDP Acts that have been enacted during the last twenty five years before returning to an examination of the role of IS personnel in the provision for PDP and their levels of awareness and commitment.
A good starting point for this research is the origins of the 1984 DPA. It was this Act that was further developed in the 1998 Act that is currently in force. Origins of the 1984 Act can be traced back to The Younger Committee of 1972 (HMSO, 1972) that looked into privacy. Ten principles were presented in the report to guide computer users in the private sector. Following this, the Lindop Committee (HMSO, 1978) examined and reported on DP.

Reasons presented for the development of the 1984 Act vary and include a concern that Great Britain would not be able to trade in Europe in the field of information services unless they complied with European Directives on Data Protection (Barber et al, 1998). This view is supported by Ian Bruce (MP for South Dorset until the 2001 general election) when he quotes a 'senior minister' as saying that 'when the UK first legislated on DP they did so because of treaty obligations' (Bruce, 2001, p23). The British Computer Society (BCS) view is that the 1984 DPA was occasioned by the Council of Europe Convention 1981 – 'which had regard to protecting individuals with regard to automatic processing of personal data' (Lewis, 1997). Shorts and de Than (1998) suggest that the 1984 Act was a response to the increasing power of computers to record and profile data. Moreover, as this power increases the consequences of errors may become more serious and there may be more of them. This is a clear recognition of a growing concern with regard to PDP.

Schedule 1 of the 1984 Act provides a set of DP principles that data users had to abide by, these were:

1. Personal data must be obtained and processed fairly and lawfully.
2. Personal data must only be used for one or more specified lawful purposes.
3. Personal data held for any purpose or purposes must not be used or disclosed in any manner incompatible with those purposes.
4. Personal data held shall be adequate for purpose(s), relevant and not excessive in relation to purpose(s).
5. Personal data must be accurate and up to date.
6. Personal data shall not be kept for longer than is necessary for purposes held.
7. Individual are entitled to (at reasonable intervals and without undue delay):
a. Be informed by any data users whether they hold personal data about an individual and how to access any such data.
b. Correct or erase incorrect data.

8. Appropriate security measures must be in place to prevent disclosure, access, alteration, or destruction or accidental loss of personal data.

Whilst the 1984 Act did bring about a focus for PDP in the UK it is possible to identify several criticisms of the Act. At a European level the response to the Convention varied; some member states did nothing whilst others did more than the 1984 Act provided for in the UK. The Confederation of British Industry (CBI) agreed with this view (Bowern, 1997, p297). The BCS report that there were considerable variations in the interpretations of the Convention by member states and that this resulted in different legal frameworks being developed with, in some cases, conflicting laws (Lewis, 1997). Other criticisms of the 1984 Act include:

1. Lack of funding to support its implementation (Raab, 1999).
2. A high number of opportunities to evade the principles of the Act through the many exemptions that were provided for.
3. The increasing ease with which 'hackers' could gain unauthorised access to data without adequate sanctions provided for in the Act (Shorts and de Than, 1998).
4. Lewis (1997) suggests that the weak definitions of 'lawful' have further undermined the 1984 Act. He goes on to add that 'the 1984 Act requires the lawful obtaining and processing of data, but does not define 'lawful' in practical terms'.
5. Bruce (2001, p23) reports the most damning criticism of the Act when he states that the government 'devised the 1984 Act to create a fig leaf that we had 'data protection' but in effect the Act did nothing to protect data’. This view is expressed as an opinion rather than as any official record, but it does serve to illustrate the low regard with which the 1984 Act has become known.

Given these reported criticisms of the 1984 Act new measures were introduced to address these (and other) issues. The ease with which some people appeared to be
able to access data led to stronger legislation being implemented to protect the rights of data subjects. Shorts and de Than (1998) argue that this awareness led to the Computer Misuse Act of 1990 (HMSO, 1990) which, for the first time, created a criminal offence for ‘hacking’. The 1984 Act applied to electronic data processing and did not apply itself to paper based files. It was increasingly apparent that this was a deficiency in the Act. Access to paper based records were increasingly provided for in response to growing demands for freedom of information. The Access to Personal Files Act of 1987 allowed subject access to ‘accessible’ information collected after the 1984 Act was passed, but it has been argued (Shorts and de Than, 1998) that it did nothing to stop ‘inaccessible’ or ‘secret’ files being kept. During the next three years legislation extended the rights that individuals had to access paper based data. These included Access to Personal Files Regulation Act 1989, Access to Medical Records Act 1988 and the Access to Medical Records Act 1990. These Acts sought to provide similar rights to those that covered electronic processing but in many cases the Acts only applied to new records. Data subjects still had fewer rights to manual than computerised data and in some cases data subjects had no automatic rights to their manually held data.

As well as a growing awareness that the 1984 Act was deficient in certain key areas, Bowern (1997, p297) suggests that it was the absence of legislation by some states in the European Union (EU), and variations in implementation of DP laws, that led to the publication of a Draft General Directive (Directive 95/45/EC) on ‘the protection of individuals with regard to the processing of personal data and at the free movement of such data’ by the European Commission in September 1990. The publications of the Directive provoked considerable debate between commercial interests and privacy advocates (Barber, 1998). In particular the direct marketing and finance industries were prominent in vocalising their concerns. The draft was further revised and published in 1992. Through extensive consultations the Directive was further revised over next three years before an agreed text was submitted to the Council of Ministers. The Directive was adopted on 24 October 1995.

Even at this early stage in the development of the current DP legislation there was consultation with representatives from professional and business organisations. The
contribution made by the CBI and the BCS on behalf of their members is taken as evidence of involvement and representation. The BCS produced the following response to the Directive (Lewis, 1997):

1. The important term 'lawful' needs to be defined and legislated for.
2. Welcomes the strengthening of the rights of the data subjects to seek compensation if they were wronged by inaccurate personal data.
3. Notes that manual systems are most likely to be paper based but will include microfiche/microfilm and include archive data held in this way.
4. The rights for data subject access requests are extended so that the data subject can not only access manual data that relates to them but also can ask for the reasons why data are being processed.
5. The Directive makes provision for the establishment of an 'In-House Data Controller'. This was particularly welcomed by the BCS and reappears in many of their communications with DP authorities and even in a personal letter to the Home Secretary (Scott, 1997).

The Chairman of the CBI Data Protection Working Group observed that the extra requirements in the Directive are (Bowern, 1997, p297):

1. Include manual data.
2. Extend activities covered by legislation to include collection, recording, organising and storage of data.
3. Specific provision requires data controllers to inform data subjects to obtain data subjects consent prior to processing.
4. Tighter conditions for processing 'sensitive data'.
5. Data subjects now have the rights to prevent lawful processing if some compelling legitimate grounds are presented and accepted.
6. The conditions under which data can be transferred outside European Economic Area (EEA) are now regulated.

Both of these contributions highlight the increasing involvement data subjects can have in the control and management of their data and its processing.
In 1995, a Government White Paper concluded that 'the time had come when those who use computers to handle personal information, however responsible they are, can no longer remain the sole judges of whether their own systems, adequately safeguard privacy' (Barber, 1998). The Government’s response to the Directive and its proposals are presented in ‘Data Protection The Government’s Proposals’ (Home Office, 1997a). Whilst that paper describes the government proposals for implementing the Data Protection Directive, it is also important in this review in that it shows evidence of another consultation event that took place. It is clearly stated in the paper that its’ intention is primarily for information but assures readers that if feedback is given by the stated date then government will have regard for the comments made. Clearly, the consultation process is being encouraged and ongoing. IS personnel contributed to the process of creating the PDP framework through their representative body, the BCS. Indeed, the post-implementation review, which itself involves a further round of consultations, was undertaken shortly after the Act came into effect.

The 1998 DPA came into force on 1 March 2000 and allowed for the incorporation of 1995 EC Data Protection Directive and for strengthening and extending the DP regime created by the 1984 Act, which it replaced.

For completeness it is worth stating the DP principles (HMSO, 1998) that underpin this Act. They are:

1. Personal data shall be processed fairly and lawfully and shall not be processed unless one of certain conditions is met.
2. Personal data shall be obtained for only one and more specified and lawful purposes and shall not be further processed or used beyond that purpose.
3. Personal data shall be adequate, relevant and not excessive in relation to purpose for which it was collected.
4. Personal data shall be accurate and up-to-date.
5. Personal data may only be kept for as long as needed for the purpose collected.
6. Personal data shall be processed in accordance with the rights of data subjects under the act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.

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

The 1998 Act covers personal data held in structured manual files; this is a new provision and given the number of Acts that emerged following the enactment of the 1984 Act no one could have been surprised by the inclusion of this form of data. The principles are similar but the 1998 Act creates some new requirements. Controllers must meet one of six conditions in order to process personal data, meet further conditions in order to process sensitive data and inform individuals when their data are collected. The Act strengthens the rights of individuals to gain access to their data and to seek compensation for wrong doings. Individuals can now prevent their data being processed in certain circumstances. They can opt-out of the data being used for direct marketing and/or fully automated decision making about them. Registration under the 1984 Act now becomes Notification. Unless exempt, Data Controllers must now inform the Information Commissioner about their processing.

Many business organisations and representative bodies provided guidance on the implications of the Act for their membership and for the business community in general. Guidance provided to small businesses identified three major changes from the 1984 Act as (Croners, 1998, p111):

1. Data held on manual records, as well as electronic, are now covered if it forms part of a structured set of data. Existing manual data is exempt for 3 years.

2. New DP principles, which data controllers have to follow, including a wide ranging provision to stop data being taken out of the EU to countries that do not have comparable, or approved, DP standards.

---

2 Sensitive data includes ethnic origins, Trade Union membership, political views and allegiance, health, sexual orientation and criminal records.
3. Some exemptions in the 1984 Act are abolished, i.e. payroll and accounts records, unincorporated members’ clubs, mailing lists and back-up data.

The BCS (BCS, 1996a) identify the main differences between the 1984 Act and the 1995 EC Data Protection Directive as being that manually stored data will be included, the requirement for notification may be simplified or exempt if data controllers appoint a Data Protection Official having defined duties and that data subjects would have greater powers to check their data and restrict its use.

These differences, whilst worthy of note in their own right, are not the main issue with regard to this discussion. They are included to show how the representative bodies of both business and the IS profession were active in providing a communications conduit between policy makers and those responsible for implementation. They were providing guidance to their members with regard to the detail of the new legislation, thus assisting them in seeking compliance. We have seen how both of these bodies were active in providing input into the consultation process and communicating the outcome of the process to their members. These findings provide some preliminary support for the view that IS personnel were involved in the process of creating the PDP framework in the UK. Representatives of the IS profession and the business community in general contributed to the process of creating the current UK PDP framework.

The discussion so far has outlined the main DP legislation that exists in the UK. It has also been shown how the process of formulating the legislation involved consultation and/or representations by both the business community and the IS profession. Before going on to consider awareness of this provision it will be worthwhile looking at other legislation that have PDP elements. The first of these, the Freedom of Information (FOI) Act 2000, is perhaps the most important and we shall see how IS personnel are identified as having an important role to play with regard to this Act.

The FOI Act (HMSO, 2000) came into force in 2000 with a phased implementations schedule spanning the following five years. Responsibility for enforcement of FOI is assigned to the IC and in doing so it is intended that a co-
ordinated and coherent approach to both sets of related legislation will emerge. The Act gives general rights of access 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.

It is worth noting here that only Public Authorities (PAs) are covered under the Act. Central and local government departments, National Health Service (NHS) organisations, schools, colleges and universities, police, Post Office, the prison service and the Parole Board are all included. The FOI Act extends rights already available under the provision of the 1998 DPA by allowing individuals to access stored information whether personal or not. The FOI Act provides two rights with regard to requests for information:

1. To be told if information exists.
2. To receive information (whenever possible) in the format requested, i.e. summary, a copy, or just to view.

Importantly, the terms of the Act were applied retrospectively once a public body is brought under the scope of the Act. A key responsibility for PAs under the terms of the Act is to create and maintain a publication scheme that must be approved by the IC. Schemes will set out:

1. The type of information the PA will publish.
2. The form it will be published in.
3. Details of any charges that may be applied to service requests for access to information.

PAs are required to provide advice and guidance to those making requests for information. Within the terms of the Act a range of exemptions exist and guidance is provided with regard to the release of information in response to a request. With regard to FOI the IC has a duty to:

1. Report directly to parliament with regard to DP and FOI.

---

3 A full list is provided as Schedule 1 of the Act (HMSO, 1998)
2. Promote good practice.
3. Assist in the preparation of and approval of publications scheme.
4. Provide information regarding public rights of access under the Act.
5. Promote and enforce compliance.

These duties are, as we will see later, very similar to the responsibilities that the IC has with regard to the DP provision.

It was stated at the start of this thesis that there is a growing awareness of PDP, it is not surprising therefore that there has been considerable legislation in the area of PDP in addition to the Acts outlined above. These include:

2. Telecommunication (Data Protection and Privacy) Regulation 1999 (HMSO, 1999)

It is worth considering these in a little more detail, however, as these are arguably less important than the legislation already discussed in ‘setting the framework’, they will be covered in less detail.

The Human Rights Act established privacy as a basic ‘human right’. The Act confers the rights for the ‘respect for private and family life, home and correspondence’. This ‘right’ has significant implications for the ‘private’ use of email within one's employment. Consideration of this need not detain us here but it is worth noting the increasing presence of PDP legislation as this may, as we shall see later, be a contributory factor in determining responses to it.

The Telecommunications (Data Protection and Privacy) Regulation 1999 was laid before Parliament on 26 August 1999 and came into force on 1 March 2000, the same time as the 1998 DPA (DTI, 1999). The regulation relates to privacy and use
of personal data in the telecom sector. Specifically the regulation limits the use of billing and/or traffic data for marketing purposes and provides subscribers with a number of new rights, such as, withholding caller ID, being left out of the directory or limiting the data included and controls over unsolicited direct marketing calls and/or faxes. An extensive consultation process was undertaken with regard to this Regulation, the details of which are publicly available (Home Office, 1999). The 1999 Regulation was enhanced several years later by the Privacy and Electronic Communications (EC Directive) Regulation 2003. This regulation provided further controls over unsolicited direct marketing sent by a range of electronic methods, including phone calls, faxes, emails and texts. The 2003 Regulation is designed to provide greater flexibility to accommodate new emerging technologies than the 1999 Regulation provided.

The Regulation of Investigatory Powers Act 2000 has come about in response to technology-enabled threats to privacy. As new and possibly more intrusive opportunities to invade our privacy develop, powers to regulate them have been provided. The most controversial part of this Act, i.e. the seizure of encryption keys, was never implemented.

The Environmental Information Regulation 2004 provides access to environmental information held by PAs, organisations or people under the control of a PA, who have environmental responsibilities. Data regarding environmental factors such as air pollution, water quality and noise are all covered under this regulation and responsibility for its implementation resides with the IC.

With regard to the legislative framework for PDP we can see that we have a comprehensive and complex provision in the UK. This will continue to develop as the technologies for privacy invasion become more powerful and the motives to use or abuse them become varied and unpredictable. Given the belief that the provision for PDP will increase and that opportunity for abuse will expand, it is now appropriate to examine in more detail the first research question identified in section 1.3: the role of IS personnel in the provision for PDP and the extent to which they are equipped to perform that role.
2.2 IS personnel, privacy and data protection

This section concerns the role of IS personnel and their responsibilities with regard to PDP. Literature exists supporting the view that IS personnel have a contribution to make in the provision for PDP, but before considering this in detail it is important to outline what is meant by the term ‘IS personnel’. The term is taken to include all of the following:

1. Systems development and/or project managers.
2. Business/systems analysts and designers.
4. Network managers, administrators and engineers.
5. Database designers, managers and/or administrators.

Other personnel with similar roles and responsibilities but with different job titles would also be included.

We can now turn our attention to a review of whether IS personnel are responsible for PDP within organisations and within systems. Starting points for this review are professional Codes of Ethics that exist within the computing industry. Bynum and Rogerson (2004, pp 169-99) present a useful summary of several leading codes and within these PDP is frequently identified as a specific responsibility of IS personnel. The authors outline the importance of privacy and legal compliance in considering the Association for Computer Machinery Code of Ethics and Professional Conduct. The Australian Computer Society Code of Ethics states that ‘I must consider and respect people’s privacy which might be affected by my work’. Finally, the British Computer Society Code of Conduct states that ‘You shall ensure that within your professional field/s you have knowledge and understanding of relevant legislation, regulation and standards, and that you comply with such requirements’. The code goes on to give PDP legislation as an example of such legislation. The Institute of Management Information Systems states that members will ‘strive to protect privacy …. of individuals’ (Bynum and Rogerson, 2004, p199). It is clear to see that these professional bodies regard PDP as a prime concern of their membership, i.e. IS personnel.
Principle seven of the 1998 DPA requires organisations to have due regard to the technical protection of privacy and data. Given the skills and expertise of IS personnel it is they that have the responsibility for providing this ‘due regard’. The IC increasingly refers to the need to embed PDP into the design of information systems. She referred to the need for an ‘ethical engineer’ applying ‘privacy enhancing technologies’ and for a merging of roles between IS personnel and others in the PDP environment with responsibilities for data (ODPR, 1997; France, 2000). Identifying IS personnel as instrumental in providing systems that facilitate PDP means that it is crucial that this group are aware of both the framework and their responsibilities within it.

The most recent Act that will be considered in this discussion specifically refers to the underpinning role of IS personnel in enabling organisations to meet their obligations. The then IC states in her introduction to the FOI Act 2000 that organisations will not be able to ‘determine their publications schemes if the presence and structure of data is not known’ (OIC, 2001). Clearly, IS personnel are instrumental in structuring and providing access to an organisation’s data resources. Raab (1999) has arrived at a similar conclusion to the IC and states that ‘those that design the systems and services with which they work are increasingly important as participants in the system’ for PDP. He goes on to add that privacy enhancing technologies (PETs) are not just a technical fix that can be applied retrospectively, but should be applied as a fundamental part of the design process. Collaborative work between the OIC and University of Manchester Institute of Science and Technology has resulted in the publication of ‘State of the Art Review’ of PETs (HiSPEC, 2002) in which a range of PETs are considered with regard to the contribution that they can make to PDP. The report authors provide practical guidelines about what PETs are, why we need them and how to use them (2002, p3). The main focus is on the technologies of anonymity, indeed this is often seen as a major contributor to PDP within systems. An early and comprehensive guide to the use of anonymity as a PET is provided by the Dutch DP Authority (Hes and Borkins, 1998 (revised 2000)). As with many other introductions to PETs the authors review the standard range of PETs that are available, but what marks out this particular review is the thorough and detailed review of the context within
which PETs can be used. The authors provide a critical evaluation of data use in the context of IS and information processing. Issues such as authentication, access control, identification, auditing and the challenges presented in a range of 'identity domains' (2000, pp23-30) are all considered in this detailed review that very much focuses on implementing PETs to support PDP as a normal IS practice.

The contribution of IS personnel is critical in designing and building systems that are compliant with existing legislation and that have the flexibility to better meet the changing and unknown requirements of further legislation. Raab goes on to report that the 'UK DPR has discussed privacy issues with ... [various large systems providers and] ... invited providers to design privacy into systems and for them to be part of the solution rather than the problem' (Raab, 1999). To support this process the IC has commissioned research into the extent to which UK based websites comply with the terms of the 1998 DPA (IC, 2002).

Members of the IS profession readily accept the responsibility to design for compliance. The Institute of Management Information Systems (IMIS) Survey's of 2002 and 2004 (Prior et al, 2003, p36; Prior et al, 2005, p21) found that 90% of respondents agreed with the statement that 'IS personnel should design systems for PDP compliance'. Evidence presented later in this thesis regarding the role of IS personnel supports the IMIS findings. Systems design is therefore seen as a key activity in the provision for PDP and this is readily accepted by IS personnel.

With regard to e-commerce start-ups, but applicable to all systems development, the lead article of 'Privacy and Data Protection' (October 2000, p1) states that 'it is important for ECommerce start-ups to be aware of DP legislation at the time when the website is created. Developing compliance after the site has been up and running may involve expensive changes that many [all] start-ups can ill afford'. IS personnel are the ones that carry the responsibility for creating these 'start-ups' and as such they need to be aware of the PDP requirements, PETs and strategies that can be employed and applied. Anton and Earp (2000) conclude their study of requirements for secure ECommerce systems by stating 'Data protection has regrettably subsisted as an afterthought when designing new systems; however, it is becoming a critical development concern'. Focusing on multimedia communications, Adams and Sasse (2001) claim that 'most invasions of privacy are not intentional but due to designers...
inability to anticipate how this data could be used, by whom, and how this might affect users’. Clear evidence is emerging that designers have a key role to play in the provision for PDP and the views of Adams and Sasse raise doubts about how well equipped they are to fulfil this role.

Lycett and Pouloudi (1999) considered ‘issues of data protection in contemporary development environments’ highlighting the ‘complex ethical debate for data controllers... the supervisory authority that oversees data protections, and information systems developers’. The literature reviewed in this thesis highlights the importance of DP in the systems development process and the plurality of professions becoming involved in its provision.

Lederman et al (2003) focused on the aim of ‘data quality’ as a privacy enhancing feature and considered the implications for information systems development. Their work adds to the growing body of evidence that supports the view that IS personnel have a contribution to make in providing PDP.

The first part of research question one was ‘what is the role of IS personnel in the provision for PDP within systems and within organisations?’ This literature review has found evidence to support the view that IS personnel are increasingly seen as key providers of PDP within systems and organisations. However there is a lack of literature regarding the precise nature of this role and/or professional practices that will bring about a greater contribution to PDP. This research seeks to provide that detail and in doing so it will answer the second research question. The research reported on in this thesis investigates whether these external requirements on the profession are recognised by members of the profession as legitimate, realistic and achievable and in doing so it goes on to seek insights into precisely how IS personnel can embed PDP into the systems they create, manage and operate.
2.3 Is the environment conducive to IS personnel contributing to privacy and data protection?

Having established that IS personnel have a key contribution to make in the provision for PDP it is appropriate to question whether or not they are equipped with the knowledge or skills to make this contribution. In order to do this a review of the available literature was undertaken and it is to the findings of that review that we now turn.

2.3.1 Awareness

This section considers the second part of research question one; how aware and accepting are IS personnel of their PDP obligations? We have seen considerable evidence of involvement and consultation and this may suggest that awareness of the provision for PDP is, or should be, high. There is clear evidence that issues that were raised during consultation are represented in the 1998 Act, but it is not clear if this is a result of the consultation process or not. The importance of IS personnel in providing for PDP is promoted significantly and evidence from the 2002 and 2004 IMIS surveys show a clear acceptance of a PDP responsibility by members of the IS profession (Prior et al, 2003, p36; Prior et al, 2005, p21). Almost 90% in both the 2002 and 2004 surveys agreed with the statement that IS personnel should ‘design PDP compliance into information systems’. These findings support an initial theoretical proposition in this research which suggests that IS personnel are increasingly seen as having a responsibility for PDP, yet they may not be fully equipped to contribute as effectively as they might. Awareness is seen as a critical factor in underpinning an effective contribution to PDP by IS personnel and it is to a detailed review of this that we now turn.

In order to assess levels of awareness this review will focus, firstly on the critical years that spanned the implementation of the 1998 Act and, secondly, the most recent data available in the 2005-2006 ICs report (IC, 2006). The 2000-2001 ‘Research Tracking Data’ (IC, 2001) shows that:
1. Using a sample of those that claim to be ‘aware of the Act’ the 2001 IC Annual Report shows that 28% of small data users and 17% of larger data users reported that they did not know how the 1998 Act applies to them.

2. With regard to the need to register, in 2000 39% of small data user and 29% of large data users did not know that they had to register. In the 2001 tracking research the question was changed to become a ‘non-prompted question’ and the impact on reported levels of awareness is significant; 88% of small and 82% of large organisations were not aware of the need to register.

3. In the 2001 Annual Report the level of spontaneous understanding of the data user obligations to data subjects are reported under six headings with an increase in understanding reported in many categories. The category showing the largest increase in awareness is the obligation that data shall not be disclosed to unauthorised recipients. For small data users the increase is from 15% in 1999 to 37% in 2000 and for large data users it increased from 30% to 40%. Whilst this is clearly a positive development it does not assure data subjects whose data is held by the more than 60% of organisations that are not aware of these obligations. Spontaneous understanding of other data user obligations are presented in table 2.1:

<table>
<thead>
<tr>
<th>Obligation</th>
<th>Large Data Users</th>
<th>Small Data Users</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1999</td>
<td>2000</td>
</tr>
<tr>
<td>Data Safe/Secure</td>
<td>18%</td>
<td>19%</td>
</tr>
<tr>
<td>Accurate/Up To Date</td>
<td>8%</td>
<td>14%</td>
</tr>
<tr>
<td>Hold no longer than necessary</td>
<td>3%</td>
<td>8%</td>
</tr>
<tr>
<td>Collect fairly</td>
<td>3%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Source: Data Protection Tracking Research 2000 (Reported in the IC's Annual Report 2001)

Table 2.1: Awareness of data users’ obligations 1999-2000

It may be reasonable to regard this as evidence of low levels of awareness concerning data users’ obligations to data subjects.

4. Levels of understanding regarding data subjects rights to see their data increased during 1998-2000 from 33% to 43% for small data users and for large data users the level of understanding have reduced from 68% to 62% during the same period. Awareness of data subjects’ rights to correct data is
significantly lower with 10% of small data users and 15% of large data users having reported awareness of this right in 2000.

5. 40% of small data users reported no understanding of individuals’ rights whilst the corresponding figure for large data users is 23%.

It is suggested that the data shows a lack of understanding and/or superficial level of knowledge with regard to DP obligations in the UK. Tracking research provides data for the last fifteen years and when examining trends it produces a positive view of developments. However, if one wanted to be a little less generous in interpretation it would be quite easy to interpret the data in a way that may cause considerable concern to privacy advocates. For example, the 2000 report shows that ‘awareness of the Act amongst the business community remains extremely high’, yet 29% of large data users and 39% of small data users did not know that they had to register. The equivalent un-prompted question from the 2001 research shows much less awareness of the need to register. Knowing ‘about an Act’ may be of little use in protecting the rights of the individual if those that ‘know’ of the Act do not have knowledge of its implications and/or their obligations to data subjects.

The 2006 Annual Tracking report isformatted differently to previous reports and, as expected, certain questions have been updated and in some cases removed. A major structural change is in the presentation of organisational data under the categories ‘public’ and ‘private’ whereas in the 2000 and 2001 data organisational data was aggregated. The 2006 report presents organisational and individual responses in separate reports whereas earlier reports did not. However, the data does continue to provide insights into the application of DP at the present time and to draw comparisons over the first five years of the life of the 1998 Act.

The data contained in the 2006 Organisations Report (IC, 2006) shows that 90% of organisations regard themselves as either ‘very’ or ‘quite’ familiar with the 1998 Act and compared to 2005 this is an increased percentage. However, organisational awareness of individuals’ rights does not show a consistent increase in awareness of specifics. The data presented in the 2006 tracking research is presented in table 2.2:
The greatest awareness within organisations concerns the rights of individuals to see their data, with almost two thirds stating awareness of this right, but beyond this right the number of organisations suggesting an awareness of other rights reduced significantly with no other right being identified by more than 20% of organisations in 2006. The right to confidentiality, a fundamental prerequisite for privacy, was identified as a right by only 20% of respondents as was the right to correct inaccuracies. Whilst acknowledging that the ‘prompted’ responses reported in the research are higher, the level or organisational awareness of individual rights continues to be low even though we are now more than six years into the post-implementation period.

The most frequently reported specific concerns that individual respondents reported are given in table 2.3:

<table>
<thead>
<tr>
<th>Unprompted</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passing on details to unknown organisations</td>
<td>45%</td>
<td>52%</td>
<td>49%</td>
</tr>
<tr>
<td>Making unwanted telephone calls</td>
<td>9%</td>
<td>18%</td>
<td>28%</td>
</tr>
<tr>
<td>Not telling me what information they hold or why</td>
<td>8%</td>
<td>18%</td>
<td>19%</td>
</tr>
<tr>
<td>Sending unwanted mail or faxes</td>
<td>14%</td>
<td>16%</td>
<td>17%</td>
</tr>
<tr>
<td>Have no worries</td>
<td>5%</td>
<td>6%</td>
<td>12%</td>
</tr>
<tr>
<td>Making decisions on incorrect information</td>
<td>13%</td>
<td>9%</td>
<td>11%</td>
</tr>
<tr>
<td>Sending unwanted emails</td>
<td>4%</td>
<td>19%</td>
<td>9%</td>
</tr>
</tbody>
</table>


Table 2.3: Concerns regarding how organisations use personal information

The reporting of individual responses starts with an acknowledgement that 63% of respondents feel that individuals have lost control over the way their data is collected and processed. This is regarded as a major concern and in particular because of the increase by 5% since 2005. With regard to accessing personal information 45% were
aware of the right but 25% were not sure of their rights. When prompted 55% agreed with the statement that ‘they were not sure of their rights’.

The organisational and individual data show that:

1. Individuals are not sure of their PDP rights.
2. A large number of individuals feel that they have lost control over the way their data is collected and processed.
3. The highest unprompted concern individuals have is that their data will be passed on to unknown organisations.
4. The least identified right reported in the organisations data is that ‘information cannot be passed on’.

Given the last of these two of these items, and the obvious tension, individuals may be right in their concerns about how well their PDP rights are safeguarded.

The research also gives an insight into the data gathering process. The research was undertaken by means of a telephone survey with the ‘data processing manager or the person responsible for computer records’ in the earlier research whilst the 2006 methodology suggests that researchers ask to speak to ‘the person responsible for deciding how information is stored and kept secure’. This could lead the researcher to IS personnel but this information is not provided. The organisational questionnaire used in the 2006 research does ask for the job title of respondents, but responses to this question are not provided in the final research report. The research explicitly sought access to the Data Controller in organisations, but it is impossible to determine the actual occupational profile of respondents. In seeking to understand the low level of awareness at an organisational level, and being generous, one could suggest that it may have been the wrong person providing the answers and that’s why awareness is low. But if the respondents are actually representative of the knowledge-base within these large organisations then it may be that those individuals that invest their data in these companies may not be served very well and it may be the IC responsibility to address this issue.

There are other responses to these questions not reported here and this is why some percentages do not equal one hundred.
Other studies show similar levels of awareness of DP issues. Barry (1998) reports ‘85% of UK companies unaware of new Data Protection Act’. The computing press reported (Phillips, 2000) that the 1998 Act is the most ‘widespread piece of IT legislation ever [and that] it seems that companies are still ignoring the Act, four months after it came into force’. The same article reports that in February 2000 ‘9 out of 10 companies did not know that the Act would come into force on 1 March’. In the 2002 IMIS survey (Prior et al, 2003, pp35-36) more than 90% or respondents felt that awareness of DP issues amongst IS personnel should be high, yet less than half of them feel that it actually is.

It is suggested that despite extensive consultations at a ‘sectoral’ level awareness amongst businesses was actually quite low and has remained so. The evidence presented above supports the view that the answer to the second part of research question one, ‘How aware are IS personnel of the PDP obligations on them and their organisations?’ is that they may not be very aware of the obligations being placed on them.

2.3.2 Commitment

In attempting to evaluate if IS personnel are committed to meeting the challenges associated with their increasing PDP responsibilities, it is necessary to look into possible explanations for the existing levels of awareness that were found during the literature review. In doing this we will provide an insight into, ‘What explanations exist for current levels of awareness?’

The process of PDP policy development and implementation will be significantly affected by the degree to which key players in the process are involved and/or support it. It was reported earlier in this thesis that IS personnel are increasingly identified as having an important contribution to make in facilitating PDP and it is this responsibility that makes an analysis of their role worthwhile in this context. If those that are increasingly identified as having a contribution to the implementation of policy are not involved in the formulation of the policy then this may significantly affect the extent to which they are aware of and committed to the
implementation of PDP legislation. This is key to the next stage of this analysis which will:

1. Review the formal policy making process.
2. Examine the opportunities that existed for involvement in the policy process by business and IS personnel.
3. Identify what involvement actually occurred.
4. Assess the extent to which involvement in the policy process affects the degree of support a professional group has for the implementation of legislation.

In attempting to examine the involvement of IS professionals in the process of policy formulation and implementation it is first necessary to be clear as to what the theoretical process is. The process of preparing for legislation at an EU level is summarised below.

The EU is the source of three main forms of legislation, directives, regulations and decisions (Rogers and Walters, 2006, p392). Directives, out of which the 1998 Data Protection Act emerged, are binding on member states spelling out what has to be achieved and by when, but leaving it up to each member state to decide how best to implement it. Notwithstanding the claims that the European legislative process is complex; for example, Rogers and Walters describe it as ‘hideously complicated’ (2006, p392), it is possible to describe the process in sufficient detail to allow for the context of the 1998 DPA to be appreciated.

Rogers and Walters (2006, p392) identify five main routes for the development of EU legislation:

1. The Council of Ministers acting without the involvement of the European Parliament.
2. The Commission makes a proposal but the European Parliament has the right to be consulted.
3. The ‘Cooperation Procedure’ within which the Commission makes a proposal but the European Parliament has the right to be consulted on the
proposal and the ‘common position’ adopted by the Council regarding the proposal.

4. The ‘Co-Decision Procedure’ in which both the European Parliament and the Council must agree on the text for it to come into force.

5. The ‘Assent procedure’ which is mainly used for international agreement and applications to join the EU.

It is plain to see how the three main European decision making institutions, the European Parliament, the Council of the European Union (informally known as the Council of Ministers) and the European Commission are all involved in the process of initiating and processing legislation at a European level (European Communities, 2003, pp10-24). Although the European Parliament is becoming more important in the EU legislative process, essentially power lies mainly with the European Commission which initiates most legislative proposals, and the Council of Ministers which eventually has the final say.

Depending on the procedure used to progress a proposal it will go through a range of consultation processes that may even involve the publication of Green Papers and subsequent White Papers documenting the process of consultation and consequent refinement of the proposal. Using the ‘Co-Decisional Procedure’ once a proposal is formally presented to the Council and European Parliament it goes through a first reading and second reading followed by a process of conciliation which either adopts the Act or not. This process is likely to include extensive consultation with interested parties. Indeed, the Citizens Guide to the EU institutions published by the EU, highlight the concepts of consultation and representation throughout its descriptions of EU processes (European Communities, 2003, pp7-22).

Once a proposal has ended its passage through the European stages and is adopted it is passed to member states to implement, in the case of a Directive, or straight into domestic law if it’s a Regulation. Regardless of which of these it is it will be communicated to the Foreign and Commonwealth Office (FCO) of the British Government as a formal document of the EU. The FCO must deposit a copy of document with the British Parliament and pass a copy to the Scrutiny Committees within two days of the documents arrival in the UK (Rogers and Walters, 2006,
The scrutiny of EU documents is done by two parliamentary committees, the Scrutiny Committee of the Commons and the EU Committee of the Lords, who between them examine approximately 1,500 documents each year of which 500 are regarded as important enough to be reported on specifically (Rogers and Walters, 2006, p395). These Committees are further divided into specialist Standing Committees and Sub-Committees so that specialist knowledge can be applied within the policy area (Dorey, 2005, pp192-3). Within ten days of a document's arrival the government department responsible for its subject matter must produce an Explanatory Memorandum that puts into the public domain details of whose responsibility for the subject matter, the legal authority under which it came into existence, the impact on UK law, policy implications, an impact assessment for UK businesses, evidence of consultations, estimates of financial implications and time-scales. When the scrutiny stage is completed a directive will then go through the normal procedures involving readings in both houses and associated revisions before being incorporated into law. The various steps described above regarding the UK role in the legislative process also provide opportunities for UK interests to be consulted.

This outline of the European and British legislative process serves to illustrate the opportunities for consultation that exist within this process. Cairns (1997, p48), who was writing at the time the 1995 Data Directive was announced, adds that 'when making policy proposals the watchword invariably observed by the Commission is consultation'. Dorey (2005, pp160-161), suggests that 'organized interests remain a key component of the policy process in Britain', adding that these groups have become 'Europeanized, with many, if not most, national-level organized interests seeking to exercise influence through the EU'. The next section considers the extent of consultation that took place between representatives of business and the IS profession and policy makers.

In this section the process of consultation relates to the European Directive 95/46/EU and to the 1998 DPA. This thesis will look at responses to both the Directive and the 1998 Act before seeking to draw conclusions regarding the process, outcomes and influence of consultation. The CBI responded to the request for consultation by stating that the proposals were inflexible, unworkable in parts
and unacceptably costly to implement (Bowern, 1997, p297). The CBI immediately set-up a working group to undertake a detailed critique and make representations as appropriate. During 1990 to 1995 the working group organised conferences, held seminars for CBI members, met with EU Commissioners and Home Office officials, appeared before the House of Lords Select Committee on Europe Committee Legislation and participated in the Union of Industrial and Employers' Confederations of Europe Working Party in Brussels. The Chairman of the Working Group reported that ‘many of the changes made to its original draft met our representations’. He also adds that ‘In spite of this the adopted Directive does still impose a more onerous regime on the UK than the 1984 Data Protection Act’ (Bowern, 1997, p298). The view expressed here is that consultation did take place, with and on behalf of, the business community.

The Directive did provide for a degree of flexibility in national implementation and as a consequence the Home Office launched a series of consultations. The CBI responded:

1. That primary legislation should replace the 1984 Act to avoid confusion.
2. The CBI welcomed the intention to restrict the application of the Act to living persons.
3. The 40 days to prepare a response to a data subject access request was supported.
4. CBI argued for exemptions for medical and/or pharmaceutical research. They also advocate that, in employment, individuals should not have access to data created for speculative planning purposes such as career or deployment planning.
5. With regard to ‘Special Cases’ they argue that data such as TU membership, occupational health, and equal opportunities monitoring should be exempt from the ‘prohibition on processing special categories’. Moreover, they also argue that private sector companies should have access to criminal records to prevent theft and fraud.
6. Regarding the new requirement covering transfers of data to countries outside the EU the CBI view was that private companies should have the

---

5 In January 2007 the name was changed to ‘Business Europe’
right to decide if they should transfer data to countries that were not on a UK approved list.

It is the stated role of the BCS Data Protection Committee to monitor both European and UK DP legislation and to represent the profession and public interest in this area (BCS, 1996b). The Committee (BCS, 1996c) identified the ‘areas of overriding importance’ as:

1. Need for primary legislation.
2. The government should expressly refer to the protection of privacy of data as the primary purpose of the legislation.
3. The Government should adopt the English text of the directive so as to ensure harmony with other legislation in Europe.
4. The definition of personal data is so broad as it stands and should be made clearer.
5. Government should adopt the concept of a personal Data Protection Official to assist compliance in organisations.

The BCS presented its concerns persistently and at every level. The issues were presented in a letter from Judith M Scott, Chief Executive of the BCS to Jack Straw (the Home Secretary at the time) regarding ‘Implementation of the EU Data Protection Directive 95/46/EC’. In the letter the Chief Executive offers support for the Directive and reaffirms the need, in the BCS view, for primary legislation and for the implementation of the provisions within the Directive to allow Data Protection Officials to support the regulatory process (Scott, 1997). Many of these issues are then further addressed in the BCS Response to the Data Protection Registrar’s ‘Questions to Answers’ (BCS, 1996d). The twelve points raised need not be listed here but the dialogue serves to illustrate close involvement by the representatives of IS personnel in the consultation process.
Once the 1998 Act was published the BCS expressed (Blackwell, 1999) its concerns as:

1. Crime and taxation exemption: Secretary of State can exempt personal data of a specified description from both subject access and the requirement to process data lawfully and fairly.
2. Deceased persons: Act only covers living persons and the BCS expressed their concerns regarding the damage to living relative of a deceased person that may result from premature disclosure.
3. Use of Secondary Legislation: The Secretary of State is empowered (through statutory instruments) to determine various detailed provisions and to authorise exemptions.
4. Harmonisation across the EU: Member states can vary their response to aspects of the provision, or to simplify aspects of it, and/or to exempt data users from certain obligations. Blackwell suggests that this may lead to confusion with damaging economic consequences.

However, it was noted that even though the BCS had a range of concerns it was supportive of the development and as such they went on record as ‘welcoming the bill’ (Blackwell, 1999).

Further evidence of consultation is found in the 3000 copies of the consultation paper that were sent out and the approximately 300 replies that were received. The most comprehensive source of information regarding the outcome of this consultation is found in the feedback provided by the Home Office to those that took part in the process. Notwithstanding the fact that data analysis may have been subject to bias in interpretation and presentation the main findings are presented below (Home Office, 1997b):

1. With regard to the legislative framework, one Act is preferred for clarity.
2. It was requested that the new Act contains precise definitions and for the new Act to resemble the existing DPA as much as possible. Precisely whether this means ‘resemble’ in terms of definitions or in terms of content is not clear in the feedback.
3. Many felt that the scope of the new Act should be extended to include the deceased even if only for a period of time.

4. Concerns were expressed over definition of what is ‘personal data’ and about jurisdiction, i.e. ‘applies to activities within the scope of European law’.

5. Most respondents requested a precise definition of the term ‘manual data’ and clear guidance of what is included within the definition. A large number of respondents wanted the government to take option to delay for twelve years before accepting this responsibility.

6. Many expressed concerns over requirement to inform data subjects where data not obtained from them but from a third party source such as, mailing list vendors and electoral registers.

7. Many requested exemptions for data they held from subject access. A frequently expressed concern focused on the need to protect third party informants and sources of data such as complainant, informers.

8. Generally agreed that 40 days for a subject access was reasonable.

9. Many respondents suggested that their processing should be exempt from all or parts of the Act. Indeed, many referred to exemptions that were provided for in the 1984 act and requested the same exemptions in the new regime.

10. Many representations from the media were forthcoming. In particular, investigative journalists sought exemptions to protect their sources and for the Act not to hamper their work. Others did not want the journalists to be given ‘carte blanche’ exemptions.

11. With regard to notifications the simplification of existing arrangements met with considerable approval. There was also considerable interest in an in-house Data Protection Official but there was little commitment to use one.

12. There was considerable support for existing enforcement mechanisms with some support forthcoming for the Data Protection Registrar (DPR) having increased powers of investigation.

13. The issue of transferring data to countries outside the EU was commented on by many respondents. The desire for certainty with regard to overseas transfers was paramount and concern was expressed over the affect on competition if a European list is not agreed.
The evidence presented so far has shown that the theoretical process for the development of European PDP legislation has been conformed to in many respects and that both business and IS personnel have been represented in the process. If we accept that the CBI and BCS were representing the views of their members and given that the process of consultation was extensive and ongoing, it may be reasonable to presume that awareness of the Act should be quite high. It is appropriate, therefore, to now consider this issue specifically.

The original premise of this research was that there is a lack of awareness amongst IS professionals with regard to PDP issues and with regard to the legislative framework in particular. It is suggested that reported levels of PDP awareness show a lack of knowledge, and therefore understanding, and that this is consistent during the period 2000–2006. Given the increasing amount of PDP legislation that has emerged and the involvement of the IS representative bodies in the policy process it is reasonable to expect awareness to be high; however, this is not the case. The focus of this discussion will now change to examine reasons for the reported levels of awareness and in doing so we shall move the focus of analysis from ‘involvement in the policy making process’ to a consideration of the ‘policy implementation process’.

It may be that the low level of awareness amongst IS professionals in the provision for PDP has more to do with policy implementation rather than policy formulation. IS professionals are often the implementers of policy and not necessarily the policy makers. It is frequently (Gerston, 1997, p111; Parsons, 1995, p462) noted that implementation of policy is often a neglected part of the whole process. It is possible that it is a lack of involvement and/or commitment to implementation that is of more interest than involvement in the policy formulation process. Reported levels of awareness may be more a consequence of implementation processes than policy formulation and as such the discussion so far may have been looking at the wrong stage of the policy process in seeking to understand levels of awareness. Before looking in to this in detail it is useful to inform this discussion by considering the formal policy implementation process.
Gerston provides a detailed and somewhat traditional review of the implementation process; this will inform our discussion of PDP policy making and implementation. He suggests that implementation is 'positioned on the less visible ‘backend’ of the [policy making] process, this component is often overlooked and undervalued' (1997, p97). If this is the case, does this apply to the EU law making process and does this contribute to the lack of awareness found in the UK? Before going on to look at some of the 'critical observations to implementation' it is worth noting that he regards ‘clear, specific and well directed policy decisions [as] essential prerequisites for implementation’. Did the 1998 Act provide that?

Gerston (1997, pp111-9) identifies the most critical factors with regard to implementation as:

1. The ability to ‘Bargain’. Once the policy is formulated the ability to modify it through ‘bargaining’ should be restricted. He goes on to add that ‘the more an implementation agency is allowed to bargain, the more it may take the policy away from purpose and aim’.
2. Secondary legislation may contribute to confusion and a corresponding reduction in awareness
3. A lack of funding is regarded as ‘a virtual guarantee of programmatic disaster at the point of implementation’.
4. Any changes in priorities may bring an implementation process to an end.
5. If there are ‘multiple goals’ (and there usually are) then implementation may be problematic. Public policies, he argues, are ‘coalition products’ in that they emerge from a cycle of consultations between often conflicting groups who have to discuss, disagree and compromise and then buy into agreed policy’. Policy is often amended to reflect the many conflicting views and if it seeks to serve too many then it may present too many conflicting goals at the same time. As policies are amended during implementation to serve ‘too many masters’ they may drift away from the original policy goals.

---

6 This section is only included to inform the consideration of the role of IS personnel in the implementation of PDP legislation. The focus is on the role of IS personnel in the process and not the actual implementation process. Given this, it is not intended to evaluate the views expressed by Gerston (1997) and Parsons (1995) with regard to the implementation process. They are included as representative of a ‘body of opinion’ that exists in this area.
6. Political support may be problematic once the policy is handed over to the bureaucracy to implement. A ‘lack of congressional [his example is American] supervision’ during the implementation phase can lead to problems.

7. Fragmentation may lead to a loss of control and difficulties in monitoring the implementation of policy when undertaken in large ‘committee based’ organisations or alliances.

Parsons (1995, p464) agrees that implementation of policy is often a neglected stage in the policy process and presents similar obstacles to those presented by Gerston; crippling constraints, availability of time and resources and the need for a clear and agreed policy being perhaps the most important ones. Dorey (2005, p198) refers to ‘prerequisites for perfect implementation’ which include, adequate resources, clear, consistent and coherent objectives, which are fully understood and/or accepted by ‘street level bureaucrats’, and that those to whom the policy is applied respond predictably and appropriately. It is worth considering this matter in a little more detail. We have seen that the process for developing a PDP framework has a thirty years history and that representatives of IS personnel and businesses in general have made extensive responses during the consultative process. If we accept that these bodies are representing the views of their members then it is reasonable to assume that some sub-sectoral consultation took place. It may be that we have an effective policy making process but other factors are affecting the implementation process and/or awareness in a negative manner.
2.3.3 Policy Networks

Given that the issue of implementation of EU directives is core to this analysis it is worth considering theory from the area of political science that seeks to inform the EU policy relationship with member states. One of the most developed conceptual tools for such analysis is that of Policy Networks (PN). A lack of PDP awareness and/or involvement in implementation of PDP legislation may be a consequence of some partially or totally ‘hidden processes’ that take place in the mediation and implementation of policy directives by relevant PN. It is to this area that we now turn our attention.

PNs are a concept that has been developed to address the role of ‘networks’ in the process of policy formulation. A PN is ‘a set of relatively stable relationships which are of a non-hierarchical and interdependent nature linking a variety of actors, who share common interests with regard to policy and who exchange resources to pursue these shared interests acknowledging that co-operation is the best way to achieve common goals’ (Börzel, 1997). The role of PNs in affecting policy outcomes is well established (Marsh, 1998, p10) and that they represent a ‘useful conceptual tools for gauging relations between public and private actors at the EU level’ is also recognised (Peterson, 1992, p229). Peterson goes on to suggest that the EU positively promotes PNs as a policy environment. Similar arguments have been put forward to explain their existence at member state level; governments like them, they regulate policy process making it more predictable and stable, they appear consultative, reduce conflict and depolitise policies and relate well to government structures and processes (Hill, 1997, p73). Indeed, some have gone as far as to suggest that PNs represent a new way of European governance in which PNs are central (Falkner, 2000, p94).

The British literature has its origins in the work of Rhodes whose views are presented by Rhodes and Marsh (1992, p9) when they suggest that PNs are a meso-level concept in two ways:

1. Emphasise the structural relationships between political institutions as the crucial element in a PN rather than the interpersonal relations between individuals within those institutions.
2. Concentrates on existence of networks at sectoral level rather than sub-sectoral.

Therefore one would expect to find networks at an aggregate rather than a disaggregated level. Rhodes and Marsh (1992, p13) restate the Rhodes classification of PN types:

1. Highly integrated policy network.
2. Professional networks that are highly stable, have restricted membership and limited horizontal articulation.
3. Inter-governmental networks.
5. Loosely integrated issue network.

Types of network can be classified by the degree to which members are integrated, types of members and distribution of resources between members.

Following the work of Rhodes, Wilks and Wright (1987, pp286-7) develop the concept of PNs by focusing more on personal relationships in the policy space and with less emphasis on structural dependencies. According to Börzel (1997), Wilks and Wright refine the Rhodes model in three ways to:

1. Stress the 'disaggregated nature of the PN in the policy sector'.
2. Emphasise interpersonal relationships as key aspects of policy networks.
3. Refine PNs into three sub-types: policy universe, policy communities and policy networks.

Whether structural, aggregate and at a sectoral level or process focused, disaggregated and sub-sectoral, what is certain is that PNs have made a huge impact on our thinking with regard to policy making. Rose (2000) has developed an argument that PNs are a truly global phenomenon and refers to the EU as a transnational PN. He does concede that as a global concept they do differ from the early definition of a PN, but he argues that they perform similar functions. Rose points out that the EU positively promotes PNs by issuing large grants each year to
bring together scholars to address transnational matters; this he argues creates transnational PN. Rose is therefore supporting the views of Peterson (1992, p229) and Falkner (2000, p94) with regard to the importance of PNs in the European policy process.

Whilst not actually presenting his work under the banner of PNs, Raab (1999) does present two related models of privacy participants and their relationships. He claims that there exists:

1. A ‘policy and implementation system or network for privacy protection’ that shapes the nature of privacy protection that is made available to us all.
2. A negotiated process to determine outcome, that is, there is not a ‘top-down prescriptive’ policy process that works in all cases.

Raab goes on to argue that the implementation of PDP policy is a dynamic political process and that the imposition of law alone may not be enough to guarantee compliance with PDP legislation. He states that ‘privacy protection [and therefore DP] has to be negotiated through various stakeholders, rather than decreed: there is a politics of data protection, not a blueprint’ (Rabb, 1999). This supports the view that networks of participants can significantly affect policy outcomes. Raab’s work is similar to the work of Wilks and Wright in that he suggests that we focus on the interaction between individuals in the policy arena with an emphasis on process. He also includes a consideration of the sub-sectoral processes.

Given this consideration of PNs in the policy formulation process it is apparent that elements may be useful in our analysis of IS personnel awareness and involvement in the PDP area. Before examining this in detail, it is prudent to look at some criticisms of PNs that have been put forward.

If a consideration of PNs is to be used to inform explanations for current levels of PDP awareness then it is important to be aware of the criticisms that have been made of PN analysis. Pratchett (1993, p8) questions the fundamental premise of Rhodes that PNs operate at sectoral levels arguing that sub-networks exist and that they are worthy of analysis because ‘they act as a filter for the changes occurring at
the macro-level, providing interpretation of these changes according to the appreciation systems for the network'. Early PN analysis focused too heavily on formal structures to the detriment of the rich interpersonal aspects of any dynamic human network. Wilks and Wright (1987, p307) sought to address this by incorporating an individual component to the network dynamic, but this proved problematic from a methodological point of view. John (1999) asks:

1. How do you measure individual preferences?
2. What are we measuring?
3. How can we measure?

He goes on to point out, with some validity, that measuring the number of contacts that exist in a PN may tell us very little. Measuring identifiable outcomes, such as this, may tell us nothing about the meaning placed on those contacts by those involved. This, it is argued, is a major weakness of the PN approach; it is the meanings that we take from interactions that influence the formulation of one's perceptions of role and responsibility. We can therefore usefully look at the role of the individual and examine their relationship and/or interaction with the PN to seek a greater understanding of the factors that affect the response IS personnel have to the PDP agenda.

John (1999) has criticised PNs in the following ways:

1. Network analysis focuses on relationships in an infinitely complex world. Accepting this would mean that the only results worth anything are those that are bound by such a restrictive set of conditions the results are not capable of replication and only exist in a theoretical case that is not reflective of real world.

2. Boundary of 'the network' in the European context is hard to define.

He goes onto quote Dowding who suggests that,

'PNs fail because the driving force of explanation, the independent variables, are not network characteristics per se but rather characteristics of components within the network. These components explain both the nature

Bargaining, and relative bargaining power, may be more important in determining the outcome of a policy process than any intrinsic value within the policy itself. This view is supported by the comments expressed by Gerston with regard to ‘bargaining’ in the policy process (see page 36 of this thesis). The PN debate has received much attention in the literature and before we go on to evaluate its potential for our purposes it is worth noting the following contribution. Dowding (2001, p102), in what one could interpret as a state of some frustration, suggests that we must attempt to ‘put an end to pointless theorising about policy networks, ‘dialectical approaches’ and (while we are at it) all the other hopelessly vague theories about the policy process such as ‘new institutionalism’.

Existing work on PNs focus on ‘policy creation’ which is not the fundamental concern of this discussion. Most of the political science research is with regard to what PNs are and their characteristics and less on the interpersonal informal bargaining interpretation that may affect policy implementation and/or outcomes. Indeed, it is suggested that the work on PNs focuses on the policy making process and references to outcomes is taken to mean the actual publication of the policy that has been influenced, or not, by the activities of a PN. The work does not focus on how a PN may operate in influencing the implementation of a policy; this is the area that this thesis focuses on.

Even though structural analysis of policy networks is becoming a little fatigued in the field of political sciences it may still have a contribution to make in our understanding in the area of PDP policy implementation. It cannot be stated, with any certainty, whether or not a PN exists that inhibits or supports the PDP policy implementation process. Given this, it is not intended to take a structural PN approach in seeking to explain levels of PDP awareness. What we will take forward, however, is a consideration of how new approaches to PN research can, and will, be used to inform the proposed research into the role of IS personnel in the provision of PDP. This is considered further in Section 3.3.2 of this thesis.
2.3.4 Role of the Information Commissioner

As the most important public official in the area of PDP it is worth considering the IC and the role of the OIC with regard to implementing PDP legislation. The role of the IC has undergone several name changes before being bestowed with the current title. During the years following the 1984 Act the role was known as the Data Protection Registrar which changed to the Data Protection Commissioner following the 1998 Act. The most recent and current change of title to IC took place on 30 January 2001. Whilst the name may have changed, the responsibilities associated with the role have expanded but, at the same time, remained somewhat constant. Since the passing of the 1984 Act Annual Reports have consistently pointed out the importance on the following as priorities for the OIC and IC:

1. Managing the implementation of several data laws, the 1984 and 1998 DPAs and the FOI Act 2000 being prominent amongst them.
2. Informing business of their responsibilities.
3. Informing the general public of their rights.
4. Enforcing the law.

Given that the IC and the OIC have sought to raise awareness for many years it is perhaps surprising that the reported level of awareness remains so low. Some possible reasons for this are considered in the next section.

Raab (1999) has suggested that a lack of funds has been a problem with regard to raising awareness. This may be the case but it is unwise to rely on this as the only source of the problem, in particular when considering the pace of change and its political context. Indeed, a potential problem that does not appear to be documented involves the pace and magnitude of legislation. The 1998 Act is a complex piece of legislation that has implications for almost all businesses in the UK and, arguably, throughout the trading world. It has been suggested that the European privacy standard (which the 1998 DPA reflects) is becoming recognised as a global landmark in privacy legislation and that it may act as a 'de facto privacy standard on the world' (Ross, 2001). Given the global implications of the Act, the complexity of the Act and its diverse and, at times, unknown audience it is perhaps not surprising that there is a
reported low level of awareness and possibly a lack of compliance to the levels hoped for.

Two areas in which the IC has been actively involved are, promoting the need to design information systems for compliance and examining the role of IS personnel in this process. It is appropriate to examine each of these in more detail.

During recent years the IC has been promoting the view that PDP is facilitated through the application of PETs in systems design (ICO, April, 2006). PETs are not necessarily novel or highly complex; physical controls and software design can significantly enhance PDP. The IC has stated that ‘conventional IS can be transformed to have a privacy-enhancing effect if they are designed in the right way’. The IC is promoting the view that a systems design philosophy can significantly enhance the protection of individual privacy through a process of ‘privacy friendly ... design’ conducted by ‘ethical engineers’. The promotion of PETs by the IC has led to funding for research into the application of PETs in the systems development process. (HiSPEC, 2002).

With regard to the then imminent enactment of the 1998 Act the Data Protection Commissioner states that ‘IT managers will have to work with other divisions, such as marketing, finance and personnel to make this [work] ... Data Protection is not just about IT – they cannot be successful by themselves’ (France, 2000). In the introduction to the FOI Act 2000 it is stated that PAs are unlikely to be able to meet their obligations to the Act without input from their IS personnel (IC, 2001). More importantly is a growing awareness that we must have proactive ‘design for privacy’ and not a reactive ‘fix for compliance’. Indeed, principle seven of the 1998 Act makes it clear that organisations are responsible for taking ‘appropriate technical and organisational measures to prevent hacking and/or data loss through systems crashes’. This is a clear IS responsibility and this is acknowledged by the IC who commissioned a study by Watts and Macaulay into ‘Best Practice in Systems Design’ (2002) and ‘PETs - State of the Art Review’ (HiSPEC, 2002).
2.3.5 Other explanations that may inform levels of awareness

So far this discussion has centred on the formal legislative process and responses to it. We have seen how an Act may take many years of consultation and consolidation before it is enacted. Following the passing of an Act a transition period is often provided for and considerable guidance is available from a range of agencies to assist those subjected to the terms of new legislation. Why then does research consistently show such a lack of response to legislation in the areas of PDP? This question prompts several possible responses that may have varying degrees of potential validity. These include:

1. The IS and business communities simply do not know enough about PDP legislation to implement it effectively.
2. The IS profession and/or the business community do know about the legislation but do not apply the legislation. Are there are some forces at work that militate against effective implementation? These may be on the part of those responsible for managing the implementation of the legislation or those that are required to actually do it.

It will be useful to examine each of these in more detail in the light of this developing discussion.

1. It has been an objective of the IC for many years now to increase the information given to public and businesses. The IC has consistently stated the objective of increasing awareness but it has been shown that awareness, and therefore compliance and involvement, is still at a relatively low level. Given that we have evidenced a considerable amount of consultation with regard to the PDP provision the lack of operational awareness is still problematic and one that would justify further research. It may be, for example, that the consultation was carried out at a very high level with little filtering down of knowledge or involvement. This would fit with the classic view of PNs. It may be that the consultation 'at the highest levels' missed the views of the smaller enterprises within which we invest so much of our data and for whom the receipt of information would have been crucial with
regard to implementation. Perhaps it is the research that gave rise to the view that awareness is low that is at fault. Certainly one can be critical of the DP tracking research methodology if one wished to do so. This would be useful if it was felt that inappropriate methodology gave rise to false assumptions with regard to levels of awareness amongst IS personnel; this is not the case and as such the results are left largely unquestioned. It is suggested here that there is enough information in the public domain for any organisation to acquire with regard to PDP, if they wished, and as such a claimed lack of awareness alone is insufficient reason for failing to comply.

2. It may be that the information dissemination process has been effective and the level of awareness is actually greater than reported in the research. It may be that there is a perceived advantage in claiming not to be aware of one’s legislative responsibilities in that if one can show that a lack of knowledge ‘is the current state of the industry’ then it may serve as an excuse for a lack of commitment or action. It may be that there is an ‘informal boycott’ of the legislation taking place and it is possible to speculate as to some factors that would support this view:

a. Given the relatively low level of complaints and low number of prosecutions under both the 1984 and the 1998 Acts businesses may regard the legislation as ‘optional’ in that the processes involved and penalties for non-compliance may be perceived as not too serious.
b. Given the pace with which new legislation has been introduced businesses may be waiting for a period of stability before ‘taking stock’ and responding only to discover that no period of stability is forthcoming.
c. A ‘perceived remoteness’ of Europe as a source of legislation may affect the implementation of legislation that originated there.
d. The long periods provided for ‘transitional arrangements’ may lead to a lack of prompt action on the part of businesses. This can be related to the issues that were raised in our earlier consideration of policy implementation. It was noted that when there exists a long time period between the passing of an Act and completion of its phased
implementation, opportunities to 'bargain' are increased with a corresponding increase in potential problems or at least exposure to the risk of inactivity.

The possible explanations put forward to account for levels of awareness are, at this time, purely conjecture. In order to gain a real understanding of the complex factors involved in this process further research needs to be undertaken and it is to a consideration of this that we now turn.

2.4 Review of research aims and questions following the literature review

Having concluded the literature review it is appropriate to now review the two research questions identified in section 1.3 and assess the extent to which the literature review has informed and/or answered them.

<table>
<thead>
<tr>
<th>Research question</th>
<th>Literature review findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What is the role of IS personnel in the provision for PDP within systems and organisations and how aware and accepting are they of their obligations?</td>
<td>The review of literature found considerable evidence that IS personnel are seen as key providers of PDP; however, there is a distinct lack of literature with regard to how this responsibility can be translated in guidelines for professional practice. Raab (1999) highlights the complex PDP matrix and the need for clarity. Hes and Borking (1998) have shown how anonymity in systems design can provide significant privacy enhancing features whilst the IC in the UK has been actively promoting the application of privacy enhancing technologies (HiSPEC, 2002; OIC, 2006). The role of IS personnel as presented in the literature is aspirational and high-level; what is lacking is detail with regard to the extent of IS personnel involvement in the provision for PDP and an insight into what they actually do and what they can do in support of PDP.</td>
</tr>
</tbody>
</table>

Evidence was found that there is a lack of awareness with
regard to the detail of PDP provision that exists in the UK. Tracking research undertaken on behalf of the IC was presented showing a consistent low level of awareness with regard to PDP. It was suggested that this low level of awareness in organisations supports the view that awareness amongst IS personnel may also be low; they are, after all 'organisational staff'. However, the literature review did not confirm that this low level of awareness is characteristic of IS personnel.

2. What aspects of IS professional practice have PDP enhancing opportunities and how widely known or applied are these? Literature was found and presented showing that IS personnel have a significant contribution to make; however, as stated above, it was also shown that the literature remains generic in nature. What is lacking in the literature is a detailed review of IS professional practice as a whole and examination of how it relates to specific PDP provision.

The implications of this are that the IS profession is currently subject to a process of role-adjustment with little professional or empirically based guidelines to support the profession as they undergo this adjustment.

The findings of the literature review provides sufficient evidence to support the view that further research is required to address the knowledge gap identified in section 1.2 and it is to a consideration of this that this discussion now turns.

2.5 Proposed research resulting from literature review

We have seen how both research questions are not fully answered by the review of the literature, but the review did confirm that IS personnel are increasingly seen as contributors to PDP within organisations. With this assurance, further research is needed to address the knowledge gap and the original research objectives which are reproduced below:
1. Establish actual levels of PDP awareness amongst IS personnel within a small number of UK based organisations.

2. Identify and explore the attitudes and perceptions IS personnel have with regard to their role in the provision of PDP and assess the impact these have on the IS development process.

3. Identify the extent to which IS personnel are aware of their legal responsibilities to use privacy enhancing technologies and strategies.

4. Identify which stages and practices within the systems development process IS personnel feel they have a PDP contribution to make.

5. Explore the relationship between Data Protection Officers (DPOs) and IS personnel in the provision for and management of PDP.

6. Improve the provision for PDP by enabling the wider distribution of examples of good PDP practice in organisations and the systems development process.

7. Encourage IS personnel to consider their role and professional practices in relation to PDP.

Before outlining the research that was undertaken to address these objectives it is necessary to undertake a thorough review of research approaches and methods. Following this, two scoping studies were designed and implemented to assess some basic presumptions regarding the literature review findings and to support the development of the larger empirical research that followed. These larger empirical studies involved a questionnaire survey regarding awareness of and attitudes to PDP which was followed by case study research in three organisations in an attempt to ascertain how these organisations and their staff are responding to the PDP challenge and to confirm or otherwise the survey findings.

2.6 Literature review conclusions

The literature review sought insights into the role of IS personnel in the provision for PDP in organisations and within the systems development process. It also went on to assess the extent to which IS personnel are equipped to meet the challenges they face. The literature review shows an increasing recognition that IS personnel are identified as key providers of PDP. It also found that reported levels of
awareness with regard to PDP are low in the business community and presumably, therefore, within the IS function as well. It was argued that this lack of awareness will limit the contribution that IS personnel can make to the provision of PDP. The involvement of IS personnel in the consultative process that accompanied the development and implementation of the current PDP regime was considered as a possible source of the reported lack of awareness. The role of the IC was also considered. The literature review finding support the development of further research to address the knowledge gap identified in section 1.2.
Chapter 3: Research Approach and Methods

Before outlining and justifying the particular research approach and methods that are used in this research it is necessary to outline the major approaches to IS research and their associated methods. Firstly, however it is useful to define some key terms:

1. The research approach is a reflection of the underpinning ontology, which in turn means the ‘rules about the nature of social enquiry’ (Pawson, 1999, p21).
2. Methodology ‘defines how we go about studying any phenomena .... it is a general approach to studying research topics that relate theories [approaches] to methods’ (Silverman, 2000, p79 and p300).
3. Jankowicz (1991, p158) defines methods as a systematic and orderly way of collecting data so that information can be obtained from those data. According to this definition methods are techniques for data collection.

For the purpose of this research the research approach gave rise to the methodology and that in turn significantly influenced the choice of methods.

3.1 The quantitative and qualitative distinction in IS research

One of the most common distinctions with regard to research approaches is the one between quantitative and qualitative and as such it is appropriate to consider this distinction.

3.1.1 Quantitative research

Quantitative research is described as being concerned with ‘collecting data about things that can be counted’ (Moore, 2000, p120). Silverman (2000, p2) adds that quantitative research is objective, value free, hypothesis testing and abstract. Quantitative research, therefore, views phenomena as measurable and capable of classification. Silverman suggests several criticisms of the quantitative approach to research:
1. Low levels of contact with respondents.
2. The risk that statistical correlations are based on arbitrarily defined variables.
3. Speculation about the meaning of correlations may rely too heavily on the application of 'un-scientific' common sense.
4. The pursuit of 'measurable' phenomena may lead to an acceptance of societal definitions and concepts.

Methods for undertaking quantitative research may include social surveys, experiments, use of official statistics, structured observations and content analysis (Silverman, 2000, p3). It is reasonable to add structured questionnaires and structured interviews to those suggested by Silverman. These methods may be seeking 'objective scientific measures' and as such they have their origins in the work of pioneering positivistic social scientists. It is also interesting to note the frequent use of the word 'structured' and in doing so it is possible to relate the methods of quantitative research with more recent developments in positivism. For most of the middle of the twentieth century positivistic research was carried out under the banner of Structural Functionalism which for the most part used the same set of methods and has in recent years been applied to IS research. (Markus, 2004, p46)

3.1.2 Qualitative research

Moore (2000, p102) describes qualitative research as being concerned with 'information about things that are less easy understood by counting them'. It emphasises a more personal approach in which detailed and meaningful insights are sought. Attitudes of IS personnel regarding their responsibilities to PDP is an example of such a qualitative insight. Silverman (2000, p8) classifies qualitative research as flexible, subjective, speculative and grounded in the subject matter. He adds that qualitative research is underpinned by the belief that a deeper and more meaningful understanding of human activity can be realised through the application of qualitative methods. Qualitative researchers have a preference for naturally occurring data, for meaning rather than pure behaviour, a rejection of the natural science method as a model and a preference for inductive hypothesis-generating research, rather than hypothesis testing (Silverman,
Qualitative research however is not without its criticisms and Silverman suggests the following:

1. Often regarded as small scale and 'preliminary, to be used before serious counting begins'.
2. Difficulty with regard to verifying results through replication.
3. Qualitative data is dependent on interpretation of action and events recorded and as such exercising control over interpretation is extremely difficult and possibly undesirable.
4. 'Anecdotalism' as a source of research data may undermine research findings due to a lack of formal research data.

Within this approach suitable methods would include un-structured and/or semi-structured interviews, observation, group discussions and natural observation, all of which can be conducted as part of case study research. Jankowicz (1991, p159) includes the following methods as qualitative: conversation; individual interview; focus group; key informant interview and repertory grid.

The emphasis in qualitative research is on the detail usually gained by the study of a small sample that is rich in meaning and insight. Silverman refers to 'qualitative data as stronger on long descriptive narrative rather than on statistical tables' (2000, p90). Followers of a qualitative approach may reflect a 'world-view' that adopts a less deterministic view of human behaviour than that supported by the positivists, whose epistemology is outlined in the next section.
3.2 The underlying epistemology of qualitative IS research

In the field of qualitative IS research the work of Myers (1997) is increasingly influential and as such it is appropriate to draw up on his work to inform this research. Myers identifies three underlying epistemologies within the qualitative framework and is it appropriate to consider these before moving on to examine data collection methods.

3.2.1 Positivism

Positivism emerged as an attempt to create a ‘positive science of society’ to explain human phenomena in the same ‘scientific’ manner that had proven so successful in the natural sciences in early nineteenth century Europe. Positivists advocated the ‘scientific method’ as the way to understand the objectively given reality (Myers, 1997). Positivist social scientists would develop a hypothesis that would then be subject to scientific testing which would either prove or refute the hypothesis. Once a ‘positive law’ had been proven by replication it was regarded as ‘fact’. Positivists believed that ‘facts’ existed and were awaiting discovery through the application of the scientific method. Positivism, with its basis in realism and empiricism (Preece, 1994, p71), exhibits a deterministic view of human behaviour. It was believed that if the same variables (people) are exposed to the same stimulus (socialisation, education, etc) they will respond in the same predictable way. How variables respond to controlled inputs was regarded as discoverable and therefore predictable. In the same way that we can discover the boiling point of water and predict that water will boil at the same temperature if all other variables remain constant, positivists believe that we can do the same with human phenomena.

The methods associated with positivistic enquiry include structured questionnaires, structured interviews, experiment and formal measurements giving rise to data that is ‘countable’ and/or measurable. This hypothetico-deductive approach relies heavily on empiricism, hypothesis testing and the production of formal testable theories of human phenomena. Issues such as objectivity and scientific measures are fundamental to positivism.
Many problems were identified with this approach during the nineteenth and twentieth centuries. The most notable include:

1. The subject matter of the social sciences is fundamentally different to that of the physical sciences. ‘People’ with free will and motives are fundamentally different to the subject matter of the natural sciences and as such it may not be appropriate to use the same approach and methods to study them.

2. The positivists portray human behaviour as ‘deterministic’ in a manner that is difficult to sustain when concepts such as ‘free will’ and ‘motive’ are considered. This has led to accusations of naivety with regard to their view of social causation (Preece, 1994 p71).

3. Stowell and West (1994, p123) suggest that positivism lacks a consideration of history in explaining current situations and that the assumption of ‘value-free methods’ is questionable.

Positivism has remained significant in social research for more than one-hundred years and it is therefore not surprising that the legacy of positivism is so pervasive that ‘knowledge claims not grounded in positivist thought are simply dismissed ... as invalid’ (Hirschheim, 1985 p.33). However, there is a research approach not grounded in positivism that has contributed significantly to IS research and it is to this that we now turn.

3.2.2 Interpretive

Interpretivism has its roots in the interactionist school of American sociology which developed as a direct challenge to the then dominant paradigm of positivism. Interactionists believed that the social world and knowledge about it was not an objective ‘thing’ waiting passively to be discovered by the application of the ‘scientific method’. Rather the social world is the result of interactions between actors and that this interaction was mediated through the use of symbols. Interactions are symbolic; they are rich in motive, meaning, complexity and are infinitely subjective. Interactionists, and in particular the symbolic interactionists, reject the objectivity of the positivists claiming that any real understanding of social phenomena can only be achieved through an understanding of the meanings placed on those phenomena by the
actors themselves. This radical departure from scientific rationalism forms the foundations of interpretativism.

Stowell and West (1994, p126) suggest that 'there is a body of researchers ...... that concentrate upon the understanding of social action based upon the actors' subjective understanding of everyday happenings rather than upon empirical data'. Accepting this theoretical foundation would imply that any attempt to understand the role of IS personnel in the provision for PDP would need to appreciate, and be sensitive to, the 'methods of enquiry' associated with the interpretive approach.

Methods that are prominent in interpretive research include semi and un-structured interviews, case study, conversations and a range of un-structured observation activities. Interpretive research provides an approach through which researchers can gain rich insights into the subjective states that underpin organisational behaviour, but some criticisms do exist. Moore (2000, pxii) identifies the following:

1. Difficulty of 'disentangling cause and effect'.
2. Measuring the degree of distortion the process of research places on the 'reality' being studied.
3. Objectivity can be difficult to maintain. Balancing the need to participate in activities and at the same time remaining objective can be problematic.
4. Interactionist researchers must avoid 'going native'. Interactionist research requires a closeness between the researcher and the subject, but there are dangers of being too close.

Other challenges for interpretive research include 'researcher bias' that may be internalised by the group being studied leading to changes in the activity being researched. Interpretive research is often small-scale and as such this limits the ability to generalise from research findings. However, this last point may not be a valid criticism; rather, it may be an enduring part of the legacy of positivism. Strategies do exist to allow generalisations to be made from qualitative data and these may overcome this claimed deficiency (Yin, 2003, p47). Popper (1979, p342) has suggested that perceptions, which are fundamental to much interpretive
research, ‘do not constitute anything like the raw material … out of which we construct either ‘experience’ or ‘science’’. Popper’s statement is firmly based in one view of what constitutes ‘real’ science; many other views exist and could be presented with equal conviction. However, it can be stated with confidence that issues such as subjectivity and the views of actors within systems are fundamental to Interpretivism.

3.2.3 Critical theory

Myers describes critical theory as focusing on:

‘oppositions, conflicts and contradictions in contemporary society, ……… and seeks to be emancipatory i.e. it should help to eliminate the causes of alienation and domination’. (Myers, 1997)

Myers suggests that critical researcher’s regard social reality as historically constituted and that it is produced and reproduced by people. Adding that their ability the change the dominant social and economic circumstances is constrained by existing forms of social, cultural and political domination. Its Marxist origins are clearly evident as are element of structural and historical determinism. Critical theory seeks human-emancipation by ‘providing the descriptive and normative basis for social enquiry aimed at decreasing domination and increasing freedom in all their forms’ (Bohman, 2005). Critical theory provides measures of effectiveness in that it should explain what is wrong with the social reality, identify actors to change it and provide clear norms for criticism and goals for social transformation that are achievable (Bohman, 2005).

Critical theory seeks to provide a useable theoretical context for qualitative research that is unbound by the concepts of ‘objective’ and ‘subjective’ methods that seek insights into small-scale interactions and the views of participants in those interactions.
3.3 Research Methods

Having discussed the three main epistemologies that underpin much of contemporary qualitative IS research it is now appropriate to look at two of the main methods used in IS qualitative research (Myers, 1997).

3.3.1 Action research

Action research 'aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration' (Rapoport, 1970, p499). Action research seeks to engage with those within the research environment to work together in an attempt to identify solutions to problems that can then be applied, or 'put into action' immediately in an attempt to solve a problematic situation.

Points worthy of immediate note are that action research is concerned with interacting with the problem situation with a view to learning about it and solving problems within it. It is an 'action' approach in two ways; firstly, it seeks to gain a subjective understanding of action, and secondly, it seeks to use the understanding gained to justify action to improve problem situations. However, action research is not just about solving practical problems; it also seeks to add to the body of scientific knowledge within the social science community (Myers, 1997). Stowell and West (1994, p128) describe this as a process in which action research feeds learning about problem situations directly back into the further development of theory. In this respect, action research is practical, professional and theoretical.
3.3.2 Case study

The aims and subject matter of this research supports the use of the case study method. Indeed, since the final piece of research reported in this thesis is a multiple case study it is appropriate to review this method in considerable detail. There are problems and challenges identified with the use of case studies such as: selecting case studies, size of case studies, industry sector, how representative of the population they are and the ability to generalise from a case study (Silverman, 2000, p103; Moore, 2000, pxiii). However, solutions and/or strategies to overcome these challenges are also forthcoming and are considered further in the detailed case study design section of this thesis (see section 5.1). Within the case study context extensive use is made of the interviewing method of fact finding.

The case study approach can be adopted when detailed insights on issues are sought from either a single or small group of organisations. Case study research can focus on a set of issues in organisations in an in-depth manner. Yin suggests that the use of a case study is a widely accepted research method that ‘investigates contemporary phenomena within its real-life context especially, when the boundaries between phenomena and context are not clearly evident’ (Yin, 2003, p13). Yin goes on to outline six types of case study research, explanatory, exploratory or description with single or multiple version of each.

The case study is regarded as a major and appropriate method used within qualitative IS research (Walsham, 1995). Myers (1997) states that ‘case study research method is particularly well-suited to IS research, since the object of our discipline is the study of information systems in organisations’ Given this suitability it is no surprise that Myers go on to suggest that case study research is the most common qualitative method used in IS research. Klein and Myers (1999) suggest that ‘case study research is now accepted as a valid research strategy within the IS research community’.

Using evidence that is forthcoming from PN research we find support for the use of the case study approach in IS qualitative research. Marsh (1998, p189) argues that the method for understanding PN dynamics is the case study and in this respect he too supports the need for detailed qualitative insights into the policy process. He states that the case study approach may serve to ‘breathe’ new life into PN study
and facilitate new insights into the processes that exist within them. His views are supported by many others in the PN field (Wilks and Wright, 1987; John, 1999; Börzel, 1997).

Case study research can be classified as either positivistic or interpretative. The positivistic case study approach is advocated and outlined by Lee (1989) and Yin (2003). The previous discussion on research epistemologies identified the main features of the positivist view of the research process; it suggests that ‘facts’ are discoverable through the application of ‘the scientific method’. Klein and Myers (1999) describe a case study as positivist if it contains evidence of ‘formal propositions, quantifiable measures of variables, hypothesis testing and the drawing of inferences about phenomena from a representative sample to a stated population’. Yin (2003, pp69-70) provides a detailed description of how the positivist approach can be used to design, undertake and evaluate case study research.

The interpretive approach to case study research is outlined by Walsham (1995). He suggests that interpretative case studies seek to contribute to our understanding of the context and processes that surround the use and development of information systems in organisations. Klein and Myers (1999) add that a case study is interpretative ‘if it is assumed that our knowledge of reality is gained only through social constructions such as language, consciousness, shared meaning, documents, tools and other artefacts’. This approach focuses on the meaning of social action as interpreted by the actors involved in the construction of that very same social action. In the interpretative case study the interpretation of events by the researcher cannot be done in isolation from the socially constructed and forever changing context, social relationships, formal and informal structures and processes.

Walsham (1995) and Myers (1997) draw our attention to the importance of the ethnographic research tradition in anthropology and how it has been applied in organisational ethnography. Data in this context is the product of our interpretation of someone else’s interpretation of what a particular reality is perceived to be. This fundamental and relatively simple statement is hugely important with regard to the nature of social action and the methods we can employ to understand it. Out of this concern Walsham draws our attention to several key issues that underpin the
interpretable tradition. Firstly, the need to be aware of the difference between 'first-order' and 'second-order' data and processes through which it changes from 'first-order' data to 'second-order' data. 'First-order' data is the interpretation of events as presented by interviewees, whilst 'second-order' data is the version of events that results from the subsequent interpretation undertaken by the researcher. Walsham adds 'Second-order concepts rely on good theory and insightful analysis, and mere collection of in-depth case study data does not provide these concepts in itself'. The second feature of the anthropological tradition that Walsham brings to interpretative IS case study is the concept of 'thick description'. In attempting to understand a complex reality that is reported through many 'interpretations' one has to seek the fullest and deepest (i.e. 'thickest') understanding before any conclusions can be reliably reported. We must seek a detailed and pluralistic understanding of any situation. Accepting one interpretation of reality too readily, no matter how closely it meets our expectations or theory, can lead to serious misunderstandings on the part of the researcher. Walsham (1995) suggests that

'the ethnographer is faced with a multiplicity of complex conceptual structures, many of them superimposed upon or knotted into one another and which must be first grasped and then rendered intelligible to others. The IS researcher entering an organisation today is also faced with complex and intertwined conceptual structures which it is difficult to grasp and make intelligible ........ The need for 'thick' descriptions is ..... important in trying to understand what is happening in connection with complex computer-based information systems, involving managers, users and designers'.

Organisational life and its artefacts are hugely complex and ever changing: seeking to realise reliable and robust 'second-order' data requires a thorough and detailed understanding of the motives and subtleties that mediate IS practice in organisations. Walsham adds that 'an IS researcher can only access these subtleties of changing interpretation by the use of approaches based on 'thick' descriptions'.

Having outlined forms that case study research can take it is worth drawing out of the discussion so far some key points regarding 'what is case study research?' Whether your approach is positivistic or interpretive case study research can:

- Be undertaken within a single case or multiple cases.
- Be positivistic or interpretive.
- Focus on ‘how’ and ‘why’ questions.
- Be empirical.
- Be related to theory.
- Provide a means of detailed analysis.
- Be supported by numerous sources of data.
- Use interviews as an important data collection technique.

Having reviewed what the case study method actually is, it is appropriate to consider when to use it.

Moore (2000) suggests that case study research can be used when:

'... it is necessary to develop a detailed understanding of what is happening in complex circumstances. Often a large-scale survey will not provide the depth of understanding required. It then becomes necessary to look in detail at what is happening in a smaller number of instances or cases. This provides greater depth at the expense of breadth.' (Moore, 2000, pxiii)

The ‘depth’ to which Moore refers would be supported by the Walsham emphasis on ‘thick descriptions’ and the need to ‘investigate contemporary phenomena in real life contexts’ as advocated by Yin.

Gratziano and Raulin (1997, p132) suggest that case studies can provide a detailed description of event, including some that may have not been identified before, and the identification of relationships amongst case study variables. Jankowicz (1991, p164) regards the greatest strength of the case study approach as being its attempt to be comprehensive, describing the full richness and variety of the subject at hand. It is the richness and detailed insights that make the case study such a valuable method. Tellis (1997) suggests that case study research strives towards a ‘holistic understanding of cultural systems of action’ which are sets of behaviours or interrelated actions engaged in by actors in social situations. Case study research according to this view is concerned with patterns of actions rather than individuals or groups of individuals.

Yin (2003, p10) has suggested that from a positivist perspective the case study method is best used when the research seeks answers to ‘how?’ and ‘why?’ questions. Walshaw, (1995) acknowledging Yin’s positivist orientation, agrees that case study
research within the interpretive framework can usefully address these types of questions.

The most frequently cited criticisms of the case study method concern the ability to generalise case study findings and the robustness of findings. Many commentators have highlighted the difficulty faced when seeking to generalise case study findings (Jankowicz, 1991; Yin, 2003; Stake, 1995). Indeed, the amount of debate that has accompanied this issue has led Yin (2003, p67) to argue that the debate is now over and need not be reviewed further. Whilst his enduring confidence in the case study method is encouraging it is still regarded as worthwhile reviewing and clarifying the main issues and assessing the extent to which they affect the research proposed in this study. Firstly, however, it is appropriate to clarify what is meant by ‘generalisability’. The concept is clearly defined by an early advocate of the positivist case study method in IS. Lee (1989) suggests that ‘generalizability is a quality describing a theory that has been tested and confirmed in a variety of situations, whether such testing is conducted through case research, laboratory experiment, statistical experiment or natural experiment’. Walsham (1995, p79) regards generalisations as being ‘explanations of particular phenomena derived from empirical interpretative research in specific IS settings, which may be valuable in the future in other organisations and contexts’. It is worth noting the use of the terms ‘empirical’ and ‘may’; the use of these two terms encapsulates the merging of positivism and interpretive approaches in a most pragmatic way.

Case study research is often accused of producing results that have little or no application to our understanding of other organisations or situations. Lincoln and Guba (2000, p27) suggest that ‘the trouble with generalisations is that they don’t apply to the particular’. In other words we can seek to generalise from our findings in one case but it rarely applies to any other ‘particular’ cases.

Many recent commentators have proposed arguments that counter the claim that case study findings are not capable of being generalised to other cases. According to Yin it is often a lack of rigour in our case study design that may lead to the claimed inability to generalise. He adds an important contribution to the debate by suggesting that ‘case studies are able to expand and generalise theories (analytical generalisation) and not
enumerate frequencies (statistical generalisation). In this way it is ‘generalising’ rather than ‘particularising’ analysis (Yin, 2003, p10); generalisation of results is done to theory and not populations of case study organisations. Yin suggests ways to increase external validity, i.e. the extent to which findings are generalisable beyond the immediate case. The more variations in places, people and procedures a case study can withstand and still yield the same results the more confidence we can have in the findings. He suggests that we can use cross-case examinations, within-case examinations and literature review findings to support and strengthen external validity.

Tellis (1997) considers the criticism that case studies cannot generalise because they are ‘microscopic’ in terms of the number of cases studies. He counters this claim by pointing out that simply increasing the number of cases studies does not change a ‘microscopic’ study into a ‘macro’ level study; it just increases the number of ‘microscopic’ studies. Yin (2003, p67) suggests that the ability to generalise case study findings is not based solely on the number of cases studies but on the rigour and integrity (internal validity) of the case study design and implementation. This issue is returned to below in the consideration of ‘robustness of findings’.

Walsham seeks to extend Yin’s views and relate them to of the types of generalisations that can emerge from interpretative case studies. Walsham (1995) identifies four types of generalisations that are possible from interpretive case studies and these are presented in table 3.1:

<table>
<thead>
<tr>
<th>Type of generalisation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development of concepts</td>
<td>Research may give rise to new insights or the development of new concepts.</td>
</tr>
<tr>
<td>Generalisation of theory</td>
<td>Concepts may exist in isolation, within the IS world or more widely. The researcher needs to see how new or changing concepts apply to existing theory.</td>
</tr>
<tr>
<td>Drawing of specific implications in particular domains of action</td>
<td>Discover the relationships between situations and ‘generative mechanisms’ that can be described and may be applied to other situations.</td>
</tr>
<tr>
<td>Contribution of rich insights</td>
<td>According to Walsham the ‘phrase is designed to capture insights from the reading of reports and results from case studies that are not easily categorised as concepts, theories, or specific implications’.</td>
</tr>
</tbody>
</table>

Table 3.1: Four types of generalisations from interpretive case studies
In the light of the preceding discussion it is suggested that the results of carefully
designed and implemented case study research can and does generalise to theory, does
assist in the development of new theoretical concepts and may, sometimes, generalise to
like cases. The criticism that case studies do not allow for generalisations is therefore
rejected.

The second major criticism of case study research regards the robustness of findings and
it is suggested that this criticism is based on a misunderstanding of the nature of case
study research. Case study research is often small scale and relatively intimate and it is
perhaps this scale and intimacy that gives rise to the view that the findings are less
reliable than those discovered through other methods. Underpinning this criticism are
concerns regarding the close relationship that may develop between the researcher and
respondents. Researcher bias and objectivity are often cited concerns. Yin (2003, p4)
addresses this issue by considering what he calls ‘Construct Validity’ which may be
questioned due to investigator subjectivity. He argues that this can be overcome by:

1. Use of multiple sources of information.
2. Establishing a chain of evidence.
3. Having the draft report reviewed by key informants.

Yin (2003, p137) also points out how ‘Internal Validity’ can increase the robustness of
findings. Internal validity refers to the robustness of the internal research design and
data analysis process. He suggests that the researcher needs to demonstrate that certain
conditions lead to other conditions, use multiple sources of evidence and convergent
lines of enquiry; all of these can increase the robustness of case study findings.

There is no fundamental reason why case study research cannot produce findings that
are robust and capable of withstanding the most rigorous review. Yin stresses the
importance of positivistic research design and documentation in defending ones
findings. Creating, publishing and applying a ‘case study protocol’ provides a public
defence against any claim that the research may not have been conducted in an
acceptable manner with valid results (Yin, 2003, p67). Lubbe (2003, p17) draws on the
work of Yin and in doing so describes a case study protocol as the detailed master-plan
for the research containing ‘full details of the case study research design, including
details of the questions to be asked, field procedures for the researcher, details of all
types of evidence required’.

Walsham (1995) and Klein and Myers (1999) provide detailed insights into how
robustness can be achieved within interpretative case studies. In presenting a set of
principles to guide IS field studies they contribute substantially to the increasing the
likelihood of producing robust findings. The principles are outlined in table 3.2:

<table>
<thead>
<tr>
<th>Principle</th>
<th>Implications for interpretive case studies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Principle of the hermeneutic cycle</td>
<td>Understanding is achieved by iterating between a consideration of the interdependent meaning of the parts and the whole they form.</td>
</tr>
<tr>
<td>2 Principle of contextualisation</td>
<td>Critically reflect on the historical background of the research setting.</td>
</tr>
<tr>
<td>3 Principle of interaction between the researcher and participants</td>
<td>Critically evaluate how ‘data’ were socially constructed and mediated between the researcher and participants.</td>
</tr>
<tr>
<td>4 Principle of abstraction and generalisation</td>
<td>Can generalise interpretive case study findings in at least the four ways described above (See table 3.1)</td>
</tr>
<tr>
<td>5 Principle of dialogical reasoning</td>
<td>Requires sensitivity to possible contradictions that may emerge between the theoretical preconceptions that guided the research design and the emerging interpretations.</td>
</tr>
<tr>
<td>6 Principle of multiple interpretations</td>
<td>Acknowledging and being accepting of the multiple interpretations that may exist of the same event.</td>
</tr>
<tr>
<td>7 Principle of suspicion</td>
<td>Be sensitive to bias and/or distortions in interpretations.</td>
</tr>
</tbody>
</table>

Table 3.2: Principles for conducting information systems field studies

Advocates of the positivist and interpretive approaches to case study research agree that
well crafted and implemented case studies are capable of producing findings that are robust and capable of verification. Yin (2003, p67) refers to the production and use of exemplary case study design to ensure that procedures used are well documented and capable of replications producing the same results. Walsham (1995, p80) states that interpretative case studies ‘if carried out and written up carefully can make a valuable contribution to both IS theory and practice’.

---

7 See Appendix 4 for the protocol that was developed to support this research.
For the purpose of this study the criticisms that case study findings are not generalisable and that they lack robustness are found to be not proven and, therefore, constitute no bar to the proposed case study research. However, the design of this research will be mindful of these criticisms seeking to identify and apply strategies to overcome them. In this way the design will ensure that the results are capable of generalisation to appropriate theory and cases. Moreover, the design will provide assurances that the research produces findings that are internally and externally robust.

In defining case study research and in considering our ability to generalise case study findings we have already encountered the issue of single or multiple cases. The researcher is faced with the choice of studying a single case study or seeking to study more than one case study. Many commentators advocate the use of a multiple case study approach. According to Yin (2003, p53) multiple case studies strengthen the results of the research and provide increased confidence in theory rather than the applicability to more cases. He goes on to add that multiple case study research is always better than relying on a single case study, with each single case being treated as a whole, with only the conclusions being aggregated. Advocates of the interpretive approach also support this view. Klein and Myers (1999) present considerable support for the view that ‘the validity of inferences drawn from one or more cases does not depend on the representativeness of the cases in a statistical sense … rather it depends on the quality of the cases and research’.

It is important to remember that in undertaking multiple case study research we are not seeking to prove that case study finding are applicable to all ‘like cases’. Nor are we seeking to provide a representative sample of cases. We treat each case as a single case using ‘replication’ rather than sampling logic where a sample is taken out of the population (Tellis, 1997). He concludes that sampling logic is inappropriate for case study research.

The role of theory is central to both positivist and interpretive research. Yin (2003, p109) places great emphasis on the role of theory in formulating research questions, guiding the data capture and analysis and in communicating the research results. Walsham (1995) offers support for the Yin view and reports that the use of theory in
any research can be classified threefold. Firstly, it can be used as an initial guide to research design and data collection. In this way the researcher can create a theoretical framework that reflects existing knowledge and serves to guide initial empirical work. The second role of theory is in supporting the iterative process of data collection and analysis. Walsham adds that:

'It is desirable in interpretive studies to preserve a considerable degree of openness to the field data, and a willingness to modify initial assumptions and theories. This results in an iterative process of data collection and analysis, with initial theories being expanded, revised or abandoned altogether.' (Walsham, 1995)

Theory in this stage of research exists to both 'inform' and to 'be informed by' the research: it is not there to constrain the research or researcher. The third role of theory that Walsham considers is that the research may inform or extend existing theory or produce new theory or concepts. These 'roles of theory' suggested by Walsham provide 'research life-cycle' coverage with regard to the contribution that theory makes to the process of interpretive case study research.

Klein and Myers (1999) seek to explain the role of theory in interpretive research and in doing so they highlight a fundamental difference between the positivist and interpretive view of theory in case study research. They suggest that in interpretive research 'theory is used in a different way than is common in positivistic research; interpretive researchers are not so interested in 'falsifying' theories as in using theory more as a 'sensitising devise' to view the world in a certain way'. Whilst differences exist between the two approaches they do share the same fundamental commitment to research driven and informed by theory which in turn further develops theory.

Having described the main features of case study research, and evaluated some of the major criticisms that are made of it, it is now possible to considering techniques that may be used for data collection in this research.
3.4 Data gathering techniques

This section outlines the major data collection methods that can be used to support qualitative IS research.

3.4.1 Interviews

Interviews allow for focused yet responsive data collection that can provide immediate feedback into the research design and subsequent interviews. Interviews have been credited with 'providing higher quality information that is [more] free from bias than many other methods' (Sharp and Howard, 1996, p147). Moore (2000, p144) develops this further suggesting that data collection and analysis should be integrated so that research findings can feed-forward into, and inform, the next research activity.

Interviews can be qualitative or quantitative in that they can be semi-structured, conversational, or highly structured. Moore (2000, p121) suggests that semi-structured interviews are best used for the collection of 'structured information and information about attitudes and beliefs'. Interview surveys are a highly structured form of interview and consist of structured questions that can be delivered in a face-to-face setting or by using the telephone (Moore 2000, p115). In between these two extremes exist a wide range of actual applications for this flexible research method. Interviews allow for complex ideas to be explored in a variety of ways according to the research design, aim and context. They are also very flexible in that the interviewer can allow the interview to change direction, vary the degree of control that is being exerted, switch from structured to unstructured and allow for new ideas to emerge and be explored. Indeed, the interviewer may get important answers and insights into questions that they had not thought to ask, but are critical to the research. If the research design permits such flexibility the interview method is potentially one of the most important methods available.

Interviews can be used alone or as part of a method-set. They can, for example follow the analysis of questionnaire data to allow for the confirmation, clarification or further development of theories or ideas. They can be used in a variety of ways
within case study research. Interviews can be undertaken with all staff or a selected few in what is known as a 'key respondent interview'. An interview schedule may group staff horizontally or vertically for interview purposes depending on the research aim and purpose. Interviews can follow a period of observation within a case study to clarify issues that have emerged using other methods.

With regard to deciding if interviews are appropriate for the research at hand Gillham (2000) presents eight questions to pose. The more positive answers one gives the more support there is for using this method. It is useful to consider these questions with regard to this research and as such they are presented in table 3.3:

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Are low numbers involved?</td>
</tr>
<tr>
<td>2  Are respondents accessible?</td>
</tr>
<tr>
<td>3  Is there a need for open questions, prompts and probing?</td>
</tr>
<tr>
<td>4  Are all respondents important to the outcome?</td>
</tr>
<tr>
<td>5  Is sensitivity and trust involved?</td>
</tr>
<tr>
<td>6  Is anonymity not an issue even though confidentiality might be?</td>
</tr>
<tr>
<td>7  Is depth of meaning central?</td>
</tr>
<tr>
<td>8  Do the research aims require insight and understanding?</td>
</tr>
</tbody>
</table>

Table 3.3: Eight evaluative questions to determine the suitability of the interview method

For this research a positive answer would be given in response to all questions with the possible exception of question four and even this is dependant on the precise research design. With regard to PNs, but equally as applicable to the provision of PDP, John (1999) suggests that researchers need to use semi-structured interviews with the main participants to ‘explore policy making and policy-adjustment processes and decisions’. Interviews in this context provide a very flexible and responsive method for seeking detailed insights into subject matter. Given the particular nature of this research and the qualities of the interview method, it is most suitable for use in this research and as such they are used extensively within the case study context.
3.4.2 Questionnaires

The major goals of a survey approach have been identified as, to ‘learn about ideas, knowledge, feelings, opinions, attitudes and self-reported behaviour of a defined population of people by directly asking them’ (Graziano and Raulin 1997, p144).

Questionnaires are a major surveying instrument and given their flexibility as a research method this is not surprising. Moore (2000, p108) suggest that their popularity stems from:

1. The relative ease with which they can be administered.
2. The flexibility to accommodate a range of research settings and purposes.
3. Their cost effectiveness.

Questionnaires are suitable for use when dealing with topics that are not contentious or overly complex. Questionnaires often provide large data sets that lack depth of detailed insights and as such they are useful for gaining an overview of particular phenomenon. However, questionnaires are often subject to poor response rates that can invalidate or undermine the ability to draw conclusions from the resulting data. Questionnaires were traditionally a postal method, but use of the Internet and email appears to be increasingly popular as a vehicle for administering questionnaires.

In creating questionnaires for survey research Graziano and Raulin (1997, p144) suggest that the following steps can be followed:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Determine the information to be sought</td>
</tr>
<tr>
<td>2</td>
<td>Define the population to be studied</td>
</tr>
<tr>
<td>3</td>
<td>Decide how to administer the survey</td>
</tr>
<tr>
<td>4</td>
<td>Construct a first-draft survey instrument, edit and refine it.</td>
</tr>
<tr>
<td>5</td>
<td>Pre-test it with a sub-sample and refine it further.</td>
</tr>
<tr>
<td>6</td>
<td>Develop a sampling frame and draw a representative sample</td>
</tr>
<tr>
<td>7</td>
<td>Administer the survey</td>
</tr>
<tr>
<td>8</td>
<td>Analyse, interpret and communicate the results</td>
</tr>
</tbody>
</table>

Table 3.4: Eight steps to questionnaire design

By following these steps it may be possible to overcome some of the better known pitfalls that exist in the use of questionnaires, but effective design is the real key.
Moore (2000, p110) suggests that the following design principles will improve the reliability of resulting data and increase response rates:

1. Inform respondents of the purpose of the questionnaire at the start and try to build in some indication of benefit to respondents for taking part.
2. Give respondents an indication of the time required to complete the questionnaire.
3. Try to portray a friendly and personal tone without being patronising.
4. Design the questionnaire to be less than four sides long.
5. Use a small number of highly focused questions.
6. With closed or restricted questions using rating-scales, limit the number of possible responses to four or six and avoid odd numbers of responses. Using a five-point scale can lead to a tendency for respondents to compromise and select the middle option.
7. Similarly, change the way questions are structured throughout the questionnaire to avoid over-familiarity occurring and responses being given without the question being read or considered fully.
8. Avoid ambiguity in the use of language; use simple words and sentence constructs.
9. Provide a space for responses that do not conform to anticipated responses.
10. Avoid biased, leading and/or negative questions.
11. Consider using ‘skips and filters’ to assist respondents to navigate through the questions.

Further guidance is offered by Thomas (1996, p121):

1. Limit the concurrent cognitive processes that your question may require to provide an answer.
2. Use concrete and specific terms rather than the abstract ones.
3. Avoid slang and professional jargon.
4. Make it clear how to navigate through and answer questions.
Mitchell and Jolly (1996, p447) emphasise the importance of establishing the format of questions in the research design. Formats such as, nominal-dichotomous, Likert-type and interval data, and open ended questions, should all be considered during the design of survey instruments.

The use of a questionnaire in this research is specifically aimed at discovering actual levels of PDP awareness, attitudes to PDP provision and how PDP is provided for within organisations. Thomas (1996, p115) regards questionnaires as useful in ‘estimating relationships between variables’. Given that this research seeks to discover actual levels of awareness of PDP and to give some preliminary insights into factors that may influence levels of awareness, the views of Thomas support the use of a questionnaire in this research.

Questionnaires are acknowledged as being suitable for fact-finding when there are a large number of respondents, when they are geographically dispersed and when it is not critical that every questionnaire is returned. Respondents for this research are drawn from the whole of the UK and potentially consist of a large number of respondents. Effective sample design will ensure that not all responses are required to enable conclusions to be drawn from the data.

Due regard was paid to questionnaire design and issues such as types of questions and responses were prominent. Once designed the questionnaire was piloted within a small sample from the respondent group. Thomas (1996, p121) suggests that piloting a questionnaire has two functions, firstly the development of instruments and procedures and secondly it serves as a ‘rehearsal of instruments and procedures’. In the proposed research the purpose of the pilot is to test that the questionnaire is meaningful and understandable to respondents and secondly, to assure that the results are suitable for extracting appropriate research data. Interviews with a sub-set of the pilot group took place to further assess the appropriateness of the questionnaire and to get respondent feedback.

A question that has not been addressed within this discussion so far concerns whether this questionnaire is qualitative or quantitative. The questionnaire has a dual purpose, firstly to establish a broad understanding of levels and patterns of
awareness with regard to PDP amongst IS personnel and, secondly to facilitate an insight into the perceptions IS personnel have with regard to their role in the provision for PDP. In this respect the first purpose can be regarded as quantitative whilst the second is primarily qualitative. However, we must remain aware of the research reality that exists between the polarised ontological positions associated with these approaches. Quantitative and qualitative may exist primarily as theoretical and analytical concepts that guide research practice rather than truly reflect it. The dual purpose of the questionnaires in the research means that it needs to support and reflect both quantitative and qualitative aspects.

3.4.3 Observation

Observation is a technique that epitomises the ontology of the interactionist approach to research. Observation may be participant or non-participant, research subjects may know about the observation or they may not, respondents may be able to give permission to be observed or may not. Clearly, this method comes with a range of ethical and methodological considerations that justify particular attention. Observation may allow for unique and detailed insights into the subjective meanings that participants in social structures and processes place on events. No other method offers the researcher the potential to get as close to research subjects as this method. This closeness may lead to insights that are impossible to gain by any other method or approach and at the same time present ethical questions that may be as important as the research itself.

Non-participant observation means that the researcher does not engage in the activity being studied whilst participative observation involves the researcher becoming involved in the phenomena being studied. Non-participative observation as a method has been widely used in psychology and social anthropology. Non-participative observation may involve the use of two-way mirrors in an attempt to reduce the degree to which the researcher’s presence distorts the essence of the reality they seek to capture and understand. Non-participant observation may be a form of structured observation.

---

8 For the purpose of this research the standard De Montfort University Ethical Review Process was undertaken and is evidenced in Appendices 1 and 2. Moreover, research ethics was also prominent in the case study design and this is reflected in the contents of the Consent Form (see Appendix 3).
as was noted earlier in this discussion. Jankowicz (1991, p159) classified structured observation as a quantitative method. This is somewhat problematic as most classification of approaches and methods would assign any form of observation as a qualitative method. His explanation of structured observation shows that the ‘observation’ is actually non-participant observation and the ‘structured’ element is structured in that the way observations are recorded, classified, and interpreted. Structured observation as presented by Jankowicz (1991, p252) is observation that is structured with regard to the practice of observation, the concepts or events looked for and the recording and interpretation of observable phenomena. This form of observation relies less on the interpretative skills of the observer and more on the ability of the researcher to classify the research domain into identifiable and meaningful concepts that are suitable for quantitative analysis.

Participant observation has a long tradition in social science and has been particularly successful in those situations where a researcher would not normally be permitted access. Haralambos (1980, p502) explains why participant observation is used in sociological studies of marginal behaviour, he states:

‘The participant observer joins the everyday routines of those he wishes to study. He attempts to observe action in its ‘normal’, ‘natural’ context. Thus he may join a group of workers in a factory or a teenage gang on a street corner; he may accompany a policeman on the beat or spend time with patients in a mental hospital’.

Haralambos provides detailed insights into the use of this method in sociology and its use may be equally valid in IS research. Both participant and non-participant observation is problematic for a number of reasons:

1. If those being studied know that they are being observed that, in effect, changes the situation being studied.
2. If they do not know they are being studied then the ethics of this need particular attention and care.
3. The skills of the researcher in interpreting observable phenomena is critical to the conclusions arrived at.
4. Over-identification with the subject may interfere with the situation being studied.
5. Measuring the degree of interference the act of observation creates and the recording and interpretation of observed data is particularly problematic.

Observing, recording and interpreting complex phenomena is fraught with methodological and procedural difficulties. These result from the complex and infinitely variable nature of the subject matter and the difficulties in determining the influence the actual process of observation has on the behaviour being observed, recorded and interpreted.

Within the IS profession systems analysts frequently use observation as a fact-finding method as part of their professional investigations into systems and processes and as such its use in IS research is wholly supportable.

3.5 Proposed research approach and method

The research described in this thesis is primarily qualitative. It uses a survey, followed-up by a case study within which interviews, discussions and document analysis are used as the main data collection techniques. In this section the approach, the case study method and data collection strategies are justified.

This research is interpretative. Creswell (1998, pp17-18) provides eight reasons for undertaking qualitative research, these are:

1. To focus on what is happening rather than why.
2. To allow for a detailed exploration of a topic.
3. To present a detailed view of a topic.
4. To understand research subjects in their own setting or environment.
5. To report research findings in a literary style using narration and storytelling.
6. To undertake research when there is less time and money available than that needed for large scale quantitative research.
7. To benefit from a willingness amongst respondents to accept the validity of this form of research.
8. To present the researcher as an active learner rather than an external expert.

It has already been suggested that methods of enquiry used in the collection of data referred to earlier in this discussion are potentially a source of difficulty in establishing a ‘true’ situation. The DP tracking research, for example, relied on telephone contacts with respondents for its data and as such its validity as representing the sum of organisational knowledge is questionable. It is suggested here that in seeking to discover and understand attitudes to PDP and compliance, telephone and other remote methods, are inappropriate. More personal, qualitative approaches are required, even if this does mean that it is only possible to study a small number of cases.

The main research methods and data collection techniques used in this research are:

1. Questionnaire. To establish a broad awareness regarding PDP awareness and practice within the IS profession and organisations.
2. Case study. Organisations will be identified for further research involving a case study approach.
3. Interviews. This will be the main fact finding method employed within case study organisations.

The approach and methods selected for use in this research fully support the research aims and objectives and, as we shall see in the forthcoming chapters, they provided an effective framework and set of procedures that were conducive to qualitative data capture.
3.6 Data Analysis Strategy

This section firstly outlines the theoretical context for data analysis and then presents and justifies the proposed strategy for questionnaire, interview and case study data.

3.6.1 Grounded Theory

Grounded theory has evolved considerably since it was first described in 1967 by Glasser and Strauss but it remains a 'bottom-up' approach to data analysis and to the development of theory (Denscombe, 2003, p109). This is important in a number of respects, firstly, it was always intended to be flexible and adaptive rather than prescriptive and restrictive and secondly it emphasizes the importance of iterative data analysis as the generative process through which theory emerges.

The data analysis undertaken in this research is informed by grounded theory and benefits hugely from the processes suggested in undertaking grounded theory analysis, but is not pure to it. Pure grounded theory would require that no prior theories exist thereby leaving the researcher open to the identification of new theory emerging untainted from the data. This research is guided by two research questions and a range of emerging and developing theoretical propositions and as such it has a preconceived theoretical position. However, grounded theory is able to accommodate such a position (Denscombe, 2003, p109).

Grounded theory generates theory as the research progresses and as such theory is grounded in the data and practice that gave rise to it. It is intuitive and close to the data, enabling theories to be tested as patterns emerge. Importantly grounded theory is strong on analysis; as Denscombe (2003, p111) points out researchers do not 'let the data speak for themselves'. It needs ongoing systematic review and comparison between the emerging data and ideas. Ho and Tan (2004, p7) support this by adding that grounded theory seeks to:

'Foster explanatory theoretical frameworks that are representative of the structures and processes observed instead of concentrating on the narration of actors.'
The ‘stories’ and views of participants are critical in grounded theory, as it is in symbolic interactionism from which grounded theory emerged and in action research where today it is widely used. The emphasis is on data analysis by the researcher and their responsibility to generate theory. Seven steps to grounded theory can be identified (Easterby-Smith et al, 1991, pp108-12) and these are listed in table 3.5:

<table>
<thead>
<tr>
<th>Step</th>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Familiarisation</td>
<td>Involves reading and re-reading data transcripts to enable reactions to the data to be noted and recorded.</td>
</tr>
<tr>
<td>2</td>
<td>Reflection</td>
<td>View reactions in the light of previous research and be informed by their theories.</td>
</tr>
<tr>
<td>3</td>
<td>Conceptualisation</td>
<td>Involves the identification of emerging themes even though their conceptual reliability is still uncertain.</td>
</tr>
<tr>
<td>4</td>
<td>Catalogue concepts</td>
<td>Label and correlate emerging themes.</td>
</tr>
<tr>
<td>5</td>
<td>Recording</td>
<td>Check the context in which different concepts were used to ensure consistency of results and analysis.</td>
</tr>
<tr>
<td>6</td>
<td>Linking</td>
<td>Join emerging patterns to form a holistic theory for review.</td>
</tr>
<tr>
<td>7</td>
<td>Re-evaluate</td>
<td>Involves the evaluation of theory based on a review by others.</td>
</tr>
</tbody>
</table>

Table 3.5: Seven steps to grounded theory

Grounded theory as applied to this research means that whilst the research commenced with a range of questions and ideas (theoretical propositions), they will be tested and revised as necessary during the research process. The proposed survey and case study research is ‘sequentially dependent’ in that the stages have to follow each other and the findings in one stage significantly affect the design of the next stage; grounded theory provides the flexible context in which this adaptation and refinement can occur. This view is supported by Denscombe (2003, p 113) who points out that:

‘Grounded theory fits neatly with the needs of researchers who are setting out to explore new territory in terms of either the subject matter of their investigations or the extent to which relevant theories have already been developed’.

This research sets out to explore new territory in terms of IS professional practice with little available in terms of a theoretical context; as such grounded theory provides the guiding framework for data analysis.
3.6.2 Data analysis of questionnaire data

Questionnaire data will be both quantitative and qualitative, with the emphasis on the latter. The data analysis strategy will be balanced accordingly. Moore (2000, pp137-40) advises on both the processing of questionnaire data and its analysis. It is appropriate to review that advice and assess its usefulness in supporting this research. With regard to processing questionnaire responses he suggests the following six steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check and verify the data.</td>
<td>Become familiar with the results by identifying standard responses and errors. These may have been identified at the questionnaire design and pilot stages, but standard errors and/or misunderstandings are always a possibility no matter how diligent the design and verification process.</td>
</tr>
<tr>
<td>2</td>
<td>Code responses.</td>
<td>Code responses to open questions into research categories to accommodate the qualitative responses. This is more effective if the questionnaire is designed for analysis as well as data capture.</td>
</tr>
<tr>
<td>3</td>
<td>Clean the data.</td>
<td>Look for errors, rogue data or inconsistencies. Again, effective design should minimise data in this category.</td>
</tr>
<tr>
<td>4</td>
<td>Produce ‘top-line data’.</td>
<td>‘Top line data’ provides a view of the responses in their most simple format, i.e. the number that answered each question and their responses. Analysis can now be carried out on the data and suggestions with regard to how this can be done are provided later in this section.</td>
</tr>
<tr>
<td>5</td>
<td>Undertake cross-tabulations</td>
<td>Bivariate analysis may lead to greater insights into the data and highlight significant internal relationships between variables.</td>
</tr>
<tr>
<td>6</td>
<td>Undertake multivariate analysis.</td>
<td>To examine the complex causal affects that variables may have on each other.</td>
</tr>
</tbody>
</table>

Table 3.6: Guidelines for processing questionnaire responses

Before assessing the usefulness of the steps provided by Moore (2000, pp141-2) to support this research, the recommendations he provides regarding analysing and interpreting the results can be presented and reviewed. Two main approaches are suggested, iterative analysis and structured analysis. Iterative analysis involves converting data into large numbers of tables and ‘cross-tabulating everything with everything else’. Moore suggests that this is not as random as first appears; look for patterns, exceptions, trends and differences seeking explanations for anomalies.
Iterations should be related to and informed by the project aims and objectives. Structured analysis begins with the aims and objectives of the research and the thinking undertaken when designing the questions. What was looked for and what was hoped to be uncovered should be recalled and key tables analysed to explore these key issues. The results may suggest other approaches or combinations of data and therefore new lines of enquiry. Trends, similarities, patterns, exceptions to patterns, explanations should be sought and ways to substantiate or explain the conclusions arrived at.

Questionnaire data produced in this research is processed in the manner outlined above in steps 1-4. These steps guide the processing of both qualitative and quantitative data and may give rise for a need to undertake bivariate and/or multivariate analysis; this will become clearer once the results are known. Both iterative and structural analysis will be used in interpreting the data.

Qualitative questionnaire data will be analysed using the principles that underpin content analysis that is considered in the following section.

3.6.3 Data analysis of case study data

In considering the analysis of case study data this discussion will firstly examine the issues surrounding the analysis of qualitative data in a general sense and then consider the strategies that are proposed for the specific analysis of case study data.

Data emerging from the use of these methods will be qualitative in nature. They will be narrative rather than numerical, they will be long descriptions of personal experiences, feelings and beliefs and they will provide a rich and detailed account of current organisational provision for PDP. Given this qualitative data we now need to consider how it will be analysed. Moore (2000, p145) presents a summary of guidelines for the analysis of qualitative data, these include:

1. Segment the data around core issues within the research, i.e. categorise it.
2. Remain flexible with regard to classification of categories.
3. Compare and contrast data from different sources.
4. Allow for the development of a personal approach using intuition.
5. Aim for high level synthesis by imposing order on the data to bring about
the identification of new themes and issues.

Points three and five support grounded theory as a theoretical foundation for the
proposed research whilst points one and two directly relate to the content analysis
approach to qualitative data analysis. Interviews and case studies produce data that
can be processed and analysed using content analysis. The following section
outlines the nature of content analysis and identifies some particular challenges
associated with its use.

Krippendorf (1980, p21) defines content analysis as 'a research technique for
making replicable and valid inferences from data to their context'. Data that can be
effectively identified and analysed by content analysis is often found in large
narrative structures that do not lend themselves to effective and detailed analysis.
Jankowicz (1991, p189) regards content analysis as the main data analysis method
associated with semi-structured interviews and its purpose in this situation is
reported as being 'to describe the content of interviews systematically'. This
systematic description is then capable of 'content analysis'. Gillham (2000) states
that content analysis is a way of 'organising the substantive context of the interview,
[i.e.] the content that is substantive'. Content analysis is used in this research to
structure the analysis of open-ended questionnaire responses, interview and case
study data.

Jankowicz (1991, p190) identifies the following stages in content analysis:

1. Identify the unit of assessment. This may be a complete expression of an idea or
   principle. Sentences or paragraphs are potential 'units of assessment' that may
   emerge in this context.
2. Choose a set of categories. These should be relative to the issues and that are
   'mutually exclusive, exhaustive and reliable'. Defining categories may be
   informed by original purpose of the research or due to emerging themes.
3. Code the material. Read the research data and assign assertions to one of the
   defined categories.
4. Tabulate the resulting data set into tables for analysis.
5. Illustrate the material. Present the categories and list their assertions.

Whilst Jankowicz's analysis is primarily concerned with semi-structured interview data, it is suggested here that the same processes can usefully and reliably be applied to the analysis of qualitative open-ended questionnaire data.

As the major part of the analysis undertaken in this research uses content analysis it is necessary to consider some problems that may be associated with this form of data analysis. The first and most apparent potential problem is the extent to which categories are defined and used. Jankowicz (1991, p191) regards this as especially problematic in areas where there are no prior research categories to guide the selection of new categories. Preece (1994, p110) suggests that the categories created for content analysis can be piloted with colleagues and/or respondents to assess their validity. He goes on to add that these pilots can be followed-up by interviews to increase confidence in the identified categories. Jankowicz (2000, p192) suggests asking others to review the data and to ask, 'would they have perceived the same categories as yourself?'. This research makes extensive use of content analysis for the analysis of qualitative data and in doing so the suggestions made by Preece and Jankowicz are accommodated into the research design. The process of identifying research codes was extensive and iterative and is described in section 5.3 of this thesis.

With regard to case study research Stake (1995, p71) suggests that 'there is no particular moment when data analysis begins'. In line with much interpretative research, interpretation, refinement and ongoing data analysis has characterised this study. However, it is useful to define what is meant by data analysis and review a range of data analysis strategies that are available to support this research.

Marshall and Rossman (1999, p150) define qualitative data analysis as 'the process of bringing order, structure and interpretation to the mass of collected data'. They go on to describe it as 'messy, ambiguous, time-consuming, creative and a fascinating process'. It is the search for evidence or inferences about the relationships between data that exists about the case(s), which they call participants 'truths'.
Many authors (Yin, 2003; Marshall and Rossman, 1999; Stake, 1995; Mason, 2002) have presented views on how qualitative data can be prepared for analysis and analysed and it is to a consideration of these views that this discussion will now turn. Once these views are explained and reviewed a data analysis strategy will be defined to support this research.

3.6.4 Suggested data analysis approach

The work of Yin (1993, 2003) has been drawn upon heavily in formulating and supporting the case study design and it is therefore logical to review his recommendations regarding the analysis of case study data. He suggests that researchers need an analytical strategy to focus the data analysis on the research questions and he proposes three general strategies (2003, pp109-14):

1. Relying on the theoretical propositions that gave rise to the case study itself is Yin’s preferred strategy. He points out that focusing on ‘How’ and ‘Why’ can serve to link data analysis to the research questions.

2. Thinking about, defining, and testing rival explanations of phenomena should be undertaken. This strategy requires that the researcher identifies alternative explanations for phenomena and tests their validity with a view to showing why the main explanation is the preferred explanation based on the evidence presented.

3. Developing case descriptions is the final general strategy presented and can be used if the two strategies outlined above cannot be made to work effectively. Yin suggests that listing and describing aspects of case studies may focus and structure subsequent data analysis.

He goes on to suggest (pp116-33) a range of specific data analysis techniques that can be used within these general strategies, these include:
Strategy | Comment
--- | ---
**Pattern matching** | This is presented as the most desirable technique adding considerable internal validity when one or more predicted patterns match empirically based patterns.

**Explanation building** | Involves analysing the case study data by building an explanation about it. Elements of the explanation may include identifying and explaining causal links that are suspected and iteration of explanation building.

**Time series analysis** | Used when an observed outcome is only possible after a number of steps or activities have been undertaken. Time series analysis involves an analysis of the steps or activities in their time sequence.

**Cross-case synthesis** | This is the final technique suggested and it involves drawing together and analysing data from more than one case. Cross-case synthesis may significantly increase the robustness of the research conclusions.

| Table 3.7: Case study data analysis techniques |

Stake (1995, p74) supports the views of Yin (2003) suggesting two ways that the researcher can attain new meaning about cases. Firstly, through the direct interpretations of an individual case instance and secondly through the aggregation of case instances until something can be said about them as an aggregation. These two suggestions correspond to ‘explanation building’ and ‘cross-case synthesis’ data analysis techniques that Yin proposes.

Given these general strategies and specific techniques Yin goes on to add some observations regarding how to undertake qualitative data analysis. He suggests that the analysis should address all three of his general strategies and especially the development of rival hypotheses and explanations. The test he suggests is that if someone can propose a rival explanation or interpretation of your data, then consider it as a rival explanation and revisit your data and analyse it further. Data analysis must remain focused on the core issues and draw upon your own skills and knowledge when undertaking data analysis thereby increasing the validity of your analysis.

Marshall and Rossman (1999, p149) suggest that data analysis involves selecting statements from the data that relate to the literature, conceptual framework and emerging research codes. As a starting point they suggest using the research questions and literature to guide data analysis, adding that qualitative data analysis is sufficient when ‘critical categories are defined, the relationship between them established and they
are integrated into an elegant, credible interpretation’. Marshall and Rossman outline a six phase analytic procedure (1999, pp152-7):

1. **Organise the data.** This involves making the data retrievable and ‘clean’.

2. **Generate categories, themes and patterns.** The authors regard this as the most intellectually challenging aspect of data analysis involving extensive reading of the data and thereby allowing for the identification of themes, recurring ideas and terms, patterns of belief and opinion. The aim is to identify the ‘subtle, tacit undercurrents’ of social and organisational life and practices. The authors refer to categories as ‘buckets or baskets into which segments of text are placed’ (p154). Drawing upon the work of Pattern (1990) these categories are further refined into ‘Indigenous Typologies’ that are created and expressed by participants and ‘Analyst-Constructed Typologies’ that are created by the researcher as they emerge from the data analysis.

3. **Code the data.** This process involves coding the identified categories and ‘marking-up’ data that matches those codes in the body of research data. In this research we may wish to adopt codes such as ‘SM’ to note material that refers to security made by a manager as opposed to ‘SD’ which could be used to identify text that refers to security, but made by a developer. Once codes have been identified the entire data set needs to be coded and new codes applied as they emerge during the coding process.

4. **Test emergent understanding.** During data analysis the researcher will become ‘closer’ to the data, more familiar and more sensitive to it. This closeness should lead to an evaluation of their developing understanding of the data. The researcher must seek out negative instances of patterns and incorporate these into the data analysis framework. They must test the data for its real relevance in contributing to a deeper understanding of the research questions and social phenomena being studied.

5. **Search for alternative explanations.** This procedure involves critically challenging patterns that may appear obvious and searching for alternative explanations which, according to Marshall and Rossman, ‘always exist’ (1999, p157).

6. **Write the report.** This final stage involves the production of a report regarding the whole research process and its outcomes.
It is clear from this review that Marshall and Rossman present suggestions that are wholly inline with the proposals of Yin. They both highlight the importance of using the original research questions to guide the data analysis and both place considerable emphasis on testing emerging and/or rival explanations for phenomena. These shared concerns are taken as evidence of the importance of these strategies.

Mason (2002, p147) presents several approaches to sorting and organising qualitative data. The two main ones are cross-sectional and categorical indexing and secondly, non-cross-sectioning data organisation. Cross-sectional indexing requires the creation of a consistent set of measures or principles for indexing the data. This process is also called ‘categorical indexing’ in that it uses classified categories to establish a common index, i.e. codes that are applied to the data consistently. She suggests several cautions that the researcher should be aware of regarding codes and indices (2002, p151):

1. Categories may be too broad to be of analytical use.
2. Often an item of data can refer to more than one category. This problem can be solved by using a serial index, which may, however become unmanageable.
3. Serial indexing cannot fully support the analysis of multi-media qualitative data and can be difficult to use for open ended interview or discussion data.

Despite these cautions Mason suggests that cross-sectional indexing can be usefully applied when:

1. Data is predominantly text based.
2. You want an overview of your data to see the coverage and scope of the data
3. You want to find and retrieve issues, topics and themes that are not apparent in ‘orderly presentation of data’.
4. You want to establish that your data addresses the underlying research questions.
5. You want to cross-reference interpretation to evidence.

Given these guidelines and associated cautions the analysis of case study data was undertaken in the following manner:
1. Restate the research questions and their corresponding theoretical propositions. This stage corresponds to the first of Yin's three strategies.

2. Identify a set of initial categories and codes. This process reflects the first two phases suggested by Rossman and Marshall and corresponds to the cross-sectional and categorical indexing that Mason suggests.

3. Read the data and code according to the initial set of codes and identify emerging (new) themes and codes. This is the third phase of the Rossman and Marshall strategy and will include sensitivity to the Yin strategy of pattern matching.

4. Segment the data to facilitate data analysis within categories. This will occur as a result of initial and ongoing data analysis. As 'explanations' and/or 'emergent understanding' develop, the data will be restructured to allow for further analysis that explicitly seeks to identify and test alternative explanations and rival theories.

5. Aggregate the findings of step four into the overall findings/conclusions. Once cross-sectional analysis has taken place the findings will be considered as a whole producing what Yin refers to as a cross-case synthesis.

3.7 Conclusion on approaches and methods

The use of a mixed set of methods in the proposed research will provide greater confidence in the findings through a process of triangulation. Triangulation is defined by Greenfield (1996, p9) as 'the process of checking if different data sources and different methods allow you to reach the same conclusion'. In this research a plurality of approaches and methods is used to facilitate triangulations and this is considered further in section 5.1.
3.8 Testing the research questions: Two scoping studies

The literature review concluded that further research was needed to establish the role and responsibilities of IS personnel with regard to PDP and the extent to which they regard this as a legitimate concern of theirs. It was also shown that awareness of PDP in organisations is low and concluded that this may include IS personnel but this was not proven. The need for further research was identified to seek additional insights into the original research questions. Before these relatively large scale pieces of research were designed and implemented two scoping studies were undertaken to test some basic presumptions and it is to a consideration of these that we now turn.

The two scoping studies undertaken at this stage of the research were designed and implemented in order to assess the validity of the literature review findings and to test the appropriateness of particular research methods. The first scoping study sought to corroborate the literature review findings and to test methods that could be used to discover levels of PDP awareness amongst IS personnel. The second scoping study also sought to corroborate the literature review findings and in addition sought to:

a. Identify which specific IS personnel have a relationship with which specific 1998 DPA principles.

b. Explore, in a more general way, the nature of the relationship between IS personnel and the 1998 DPA principles.

3.8.1 Scoping study 1 - Levels of awareness

In order to ascertain levels of awareness amongst IS personnel working in UK organisations a small-scale survey was undertaken using a respondent sample from the alumni of postgraduate computing programmes at De Montfort University. The sample used for this small scale survey may not be representative of the IS profession as a whole, however, the purpose of the survey was to seek preliminary assurances regarding levels of awareness. Forty questionnaires were sent out and fourteen useable responses were received. The results, which are reproduced in table 3.8, show an acknowledgement of the need to consider PDP in IS professional practice but a low level of awareness of specific PDP issues. The following table presents the responses received:
<table>
<thead>
<tr>
<th>Question</th>
<th>% answering positively</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you aware of a growing need to consider privacy/data protection in the IS area?</td>
<td>100</td>
</tr>
<tr>
<td>Do you work in the IS business?</td>
<td>86</td>
</tr>
<tr>
<td>Do you and your colleagues consider privacy and/or data protection in systems design?</td>
<td>71</td>
</tr>
<tr>
<td>Have you heard of the 1998 Data Protection Act?</td>
<td>93</td>
</tr>
<tr>
<td>Have you heard of the Freedom of Information Act 2000?</td>
<td>79</td>
</tr>
<tr>
<td>Do you design systems?</td>
<td>36</td>
</tr>
<tr>
<td>Do you know how many ‘principles’ there are in the Act?</td>
<td>36</td>
</tr>
<tr>
<td>Do you know what a Subject Access Request is?</td>
<td>29</td>
</tr>
<tr>
<td>Do you know when 1998 Data Protection Act came into force?</td>
<td>50</td>
</tr>
<tr>
<td>Do you know how the 1998 Human Rights Act relates to privacy?</td>
<td>29</td>
</tr>
<tr>
<td>Do you know when the FOI Act 2000 came into force?</td>
<td>29</td>
</tr>
<tr>
<td>Are you aware of the purpose/content of the FOI Act 2000?</td>
<td>36</td>
</tr>
</tbody>
</table>

Table 3.8: Scoping study 1: Questionnaire responses

3.8.2 Data Analysis: Scoping study 1 – Levels of awareness

Observations that can be drawn from these results that inform this discussion are:

1. The first three questions show that there is considerable awareness of the need to consider PDP. The 100% positive response to question one is clear evidence of this.

2. The next two questions ask if respondents have heard of the 1998 DPA and the 2000 FOI Act and again most respondents reported that they had heard of the legislation. These two questions provide confirmation for the conclusion reported in point one that there is a growing awareness to consider PDP issues; if this was not the case then the number being aware of the new legislation may well have been lower.

3. Awareness of detail is relatively low. For the most part only one third of respondents were aware of specific detail with regard to the legislation, for example details concerning purpose, the DP principles and subject access to data.
These findings are consistent with the evidence presented and conclusions drawn at the end of the literature review with regard to levels of PDP awareness. IS personnel are aware of the need to consider PDP but, based on this evidence, they may not have sufficient knowledge of the detail to discharge that responsibility as effectively as they may. This may mean that they cannot, at present, meet the objectives set by the IC of becoming a key player in developing privacy sensitive systems. The reality of the ‘ethical engineer’ is perhaps not yet with us.

If the scoping study provides useful evidence, it shows a low level of awareness of the obligations businesses have to data subjects and that constitutes a threat to the PDP rights of individuals. Moreover, the low level of awareness that currently exist may serve to undermine any future legislation in the area of PDP. If low levels of awareness, and potentially low levels of compliance, with regard to PDP is interpreted as an ‘acceptable level of compliance’ to the IS and business communities, future legislation may be undermined before it is passed. This must be regarded as undesirable.

The literature review found evidence that levels of awareness within organisations were low and this scoping study now provides evidence that this situation is characteristic of elements of the IS profession in particular. The scoping study provided evidence to support the development of a larger research study.

3.8.3 Scoping study 2 - Role of IS personnel

The aim of this second scoping study is to investigate the actual role of IS personnel in the provision for PDP. The literature review findings confirmed a belief that IS personnel are increasingly identified as having a key contribution to make; what was lacking was the detail of what that contribution actually is or can be. Using ‘personal identifiers’, anonymising data and designing for compliance have all been suggested as high level solutions to particular PDP challenges (Hes and Borking, 1998; ODPR 1997; Raab, 1999). This scoping study was designed to confirm or refute the view that IS professional practice and activities can be matched to specific PDP principles. If this could be done then it would be possible to refine and develop the scoping study and its instruments into a full study with a view to providing detailed guidelines for the IS
profession on how they can contribute to the provision of PDP within systems and organisations. What follows is a description of the scoping study and a consideration of its key findings.

The research instrument was designed to allow respondents to explore the specific contribution that IS personnel can make to PDP during their professional practice. They were required to:

1. Identify up to eight ‘IS roles’ that may exist within the broad term ‘IS personnel’.
2. For each of these roles they were required to identify the specific tasks and/or activities that someone in that role would be reasonably expected to perform.
3. Once this had been done they were required to map relationships between the ‘tasks and activities’ to the ‘DP principles’ of the 1998 Act that someone in that role could support or contribute to. The technique used for this was borrowed from entity relationship modelling in that participants were asked to draw a line from a ‘role’ to a ‘DP principle’ and to name the relationship. An example will serve to illustrate this:

```
Systems Analyst: Identify data required for purpose(s) only
Principle 4: personal data shall be adequate, etc
```

In this example a relationship is documented between the role of systems analyst and the identification of data required to fulfil some systems requirement. The contribution of the systems analyst is to ensure that excessive data is not captured in relation to the purpose(s), i.e. principle four of the 1998 DPA.

The activity that produced the data was undertaken in small student groups of between three and five members in each. All those involved in this scoping research had been in industry for the previous year and as such they all have some recent awareness of the roles and responsibilities of IS personnel. In total twelve student groups contributed to the exercise. Prior to setting the task as a student activity a small group of IS academic staff piloted the exercise to ensure that it was possible to map from 'role' to 'principle' and the results of this group activity is also included in the data presented. Table 3.9 shows the frequency with which particular IS roles are identified as having a contribution to make in the provision for PDP.
Table 3.9: Scoping study 2a: IS roles that can contribute to DP principles
3.8.3.1 Data Analysis: Scoping study 2a – Which IS personnel and which principles?

The clear outcome of the exercise is that respondents were able to link from IS role to DP principles. This is significant in that if relatively inexperienced entrants to the IS profession can provide some of the detail lacking in so much of the literature then the opportunity to fill this knowledge gap is immediate and apparent.

The high number of respondents identifying programmer/software engineers as having a contribution to make may be more a reflection of the standing of the respondent group than a real reflection of the contribution groups can and/or should be making. The students are final year computing students that had recently completed a placement year in industry. It is quite likely that many of these were recently in positions that had a title that included programmer/software engineer as part of their job description. Moreover, even if this group were not personally involved in the production of code it is possible that the level of the organisation they were operating at may include a substantial focus on the production of code. In any event they have produced suggestions that would support the view that programmers have a significant role to play in the provision of PDP in systems development.

The higher the role in a presumed IS professional hierarchy, the more general the relationship with the principles becomes. Many respondents identified job titles with the word ‘Manager’ in them as far more likely to be associated with all eight principles rather than specific principles. Whilst this may appear to lack detail it does hint to an important contribution that these staff can make; their ability to affect overall PDP provision is much higher and therefore, potentially more important, than being able to assure compliance with one or more principles. It is in this area that the real impact can be made by the IS profession.

Respondents were required to create associations between IS personnel and PDP by linking ‘IS role’ to tasks performed and then to DP principles. It would be equally valid to take a systems development life cycle (SDLC) approach to the study. This would involve agreeing ‘life cycle models’ and examining what activities are carried
out at each stage and then identifying the PDP checks or principles that could be applied at each stage. A greater degree of confidence in the outcomes would be provided if the identification of associations from two different perspectives resulted in the same relationships emerging. This matter is considered further in Chapter 4 as part of the questionnaire data analysis.

This analysis shows that particular IS roles can be identified that carry with them particular responsibilities for supporting the provision of PDP within their professional practice. The next section of this thesis provides some insight into what that actual contribution can be. This is presented in table 3.10 and discussed in the next section.
Rate at which principles are associated with IS/IT staff

1. Personal data shall be processed fairly and lawfully and shall not be processed unless one of certain conditions is met.
2. Personal data shall be obtained for only one and more specified and lawful purposes and shall not be further processed or used beyond that purpose.
3. Personal data shall be adequate, relevant and not excessive in relation to purpose for which it was collected.
4. Personal data shall be accurate and up-to-date.
5. Personal data may only be kept for as long as needed for the purpose collected.
6. Personal data shall be processed in accordance with the rights of data subjects under the act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred to a country or territory outside the EEA unless they ensure adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data.

1998 Data Protection Principles

Table 3.10: Scoping study 2b: DP principles supported by IS staff
3.8.3.2 Data Analysis: Scoping study 2b - The nature of the relationship between IS personnel and the 1998 DPA principles.

When reviewing the data presented in the table above some immediate observations include:

1. All principles are associated with IS personnel.
2. Principle seven has the highest number of associations.
3. Principles three, two and four are the next most frequently associated with IS personnel.
4. Principles one, five and eight are the least well supported.

Principles seven and three are most frequently associated with IS roles. Combining this with the conclusions drawn from the analysis of which staff are most involved we could tentatively conclude that software engineers, database administrators, project managers and systems analysts are the staff with the greatest contribution to make and the principles that they may contribute to with greatest ease are principles seven and three. The research basis of this conclusion is tentative but if following replication and subject to greater validation it was found to be valid, it would be a significant finding indeed.

Many respondents felt it important to include certain staff without being able to define any one-to-one associations between their role and the DP principles. A common observation was that some IS roles have a responsibility for managing others that have the direct ‘one-to-one’ relationship with the principles. The relationship between these personnel and the DP principles is managerial, and by proxy. To examine this relationship further it is worth looking at those roles with ‘1-8 inclusive’ identified as the relationship and examine the number of such associations they have. This is presented in table 3.11:
Two groups emerge with a significant and generic association with the DP principles. Roles with the word ‘manager’ included in their title are identified as having a generic relationship with all principles and as such their contribution is worthy of closer examination. It was suggested earlier that some IS personnel exercise their responsibilities to PDP via proxy or through managerial direction. The relationship between IS managers and the DP principles is significant in two respects. Firstly, a high number of associations are generic and secondly they have a high number of associations. Based on this small sample a large majority of the associations for those classified as ‘managers’ were of the generic ‘1-8 inclusive’ type. These findings provide tentative support for the view that IS Managers have a significant contribution to make to the provision for PDP and that their contribution is generic in nature in that they have a contribution to make in supporting all DP principles.

The data also identifies a second group worthy of particular attention, IT Support/Help Desk Staff and IT Consultants. These groups were only identified as having generic associations with the principles, all of their associations were of the ‘1-8 inclusive’ type. Respondents reported that these staff were perceived as having roles that were characterised by a high degree of interaction with and awareness of other IS personnel, systems, departments and organisations. This, it was felt, gave them a unique insight into PDP practice across many systems and settings from which they could disseminate good practice regarding all the principles. IT consultants were seen as offering strategic support for all principles whereas IT support staff were seen as contributing to PDP education and policing.

<table>
<thead>
<tr>
<th>Job Title/Role</th>
<th>No of associations</th>
<th>No of 1-8 inclusive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programmer/Software Engineer</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>Systems Analyst/Business Analyst</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>IT Support/Help Desk Staff</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>IT Consultant</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IT Manager/IT Security Manager/etc</td>
<td>13</td>
<td>10</td>
</tr>
<tr>
<td>Systems Tester</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Systems Designer/Web Designer</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>IT Training Staff</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 3.11: IS Roles with generic associations with data protection principles
Staff not listed above did not have any reported general associations with all eight principles; amongst the respondents their role and association with principles was given as more specific and identifiable.

3.9 Scoping studies, research questions and the relationship to further research

The literature review, and the scoping research that emerged out of it, provide some preliminary answers to the original research questions. These are outlined below:

<table>
<thead>
<tr>
<th>Research Question</th>
<th>Preliminary answer and evidence from literature review and scoping research</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What is the role of IS personnel in the provision for PDP within systems and organisations and how aware and accepting are they of their obligations?</td>
<td>The literature review showed that the role of IS personnel is increasingly acknowledged at a general level but there is a distinct lack of detail regarding the specific relationship between IS personnel and the provision for PDP. The second scoping study showed that it is possible to define what aspects of IS professional practice can be used to enhance PDP within systems and organisations. The study also provided a preliminary indication that the specific IS personnel that can contribute most to PDP include, programmers, IT managers and Systems Analysts and the principles they can support most include principle seven, two, three and four.</td>
</tr>
</tbody>
</table>

The literature review found evidence that low levels of awareness with regard to PDP are reported within organisations. The first scoping study provides evidence that this was also true of the sample of IS personnel that responded to this study.
2. What aspects of IS professional practice have PDP enhancing opportunities and how widely known or applied are these?

The second scoping study suggested that it is possible to identify aspects of IS practice and roles that can be supportive of PDP. What remains unknown, however, is the degree to which these are widely known and/or applied. Further research is undertaken to address this and this research is reported on in the following chapters of this thesis.

The two scoping studies reported on in this section provide confirmation of the literature review findings and provide assurances that the proposed research has sufficient focus and scope to contribute to the body of IS knowledge and to support IS professional practice. It is to a consideration of this research that we now turn.

We have seen how the literature review provided evidence that IS personnel have role to play in the provision of PDP and that current levels of awareness are generally low. Two scoping studies confirmed the literature review findings and added further insights into the complex provision for PDP. The literature review and scoping studies provide assurance of the need for research into the provision for PDP and the role of IS personnel. The research that followed sought to:

1. Empirically establish levels of awareness with regard to PDP amongst IS personnel in organisations.
2. Seek explanations for actual levels of awareness found.
3. Identify the role that IS personnel currently perform in the provision for PDP within organisations and in particular explore the relationship between Data Protection Officers (DPOs) and IS personnel in the provision for and management of PDP.
4. Identify the stages or activities within IS professional practices that have PDP enhancing opportunities.
5. Gain insights into the views of IS personnel with regard to their role in providing for PDP.
6. Identify and document a range of professional strategies that can be applied to the process of information systems development to enhance PDP.

7. Document and disseminate good practice in the area of PDP and IS practice.

These ‘objectives of future research’ are wholly in line with the original research aims, questions and objectives as stated in chapter one of this thesis. The research that was implemented following the scoping studies took the form of a questionnaire survey and case study research with the outcome of the survey feeding into the design of the case study research. The development, application and analysis of the questionnaire and its resulting data sought to discover actual levels of awareness and insights into the nature of PDP provision and insights into how IS personnel feel about their role in the provision for PDP.

The aim of the case study research is to further identify and classify perceptions and attitudes that IS personnel have with regard to their role and responsibilities for PDP. It explores the relationship between those involved in the provision for, and management of, PDP. This builds upon the results of the survey research and provides detailed insights to further inform the quantitative data that was produced as part of the survey research. The association between IS professional practice and PDP principles will also be investigated further within the case study organisations. The 'rich' data emerging out of the case study research facilitates a greater understanding of the perceptions that IS personnel have with regard to their role in the provision for PDP.

The overall synthesis of both survey and case study findings are considered in chapter 6.
Chapter 4: Survey – Levels of Awareness and IS personnel in the provision for PDP

4.1 Research Questions and methodological issues

In addressing which IS personnel and what systems development activities present PDP enhancing opportunities a survey of IS personnel was designed and undertaken. The survey sought the views of IS personnel with regard to their role in the provision for PDP. The survey also sought the views of IS personnel regarding which staff can contribute to PDP and at what stage of the systems development process that contribution can be made. The survey served as a vehicle through which insights were sought into actual levels of awareness, attitudes to PDP provision and about how PDP is provided for within organisations. The use of a questionnaire at this stage of the research and the associated data analysis strategy were proposed and justified in sections 3.4.2 and 3.6.2 of this thesis and as such they are not repeated here. However, it worth pointing out that the number of respondents to the questionnaire (59) and the focus on qualitative data analysis do mean that detailed statistical procedures are inappropriate in supporting the qualitative analysis of the survey results. It is however, necessary to include a brief review of the procedural aspects of the questionnaire design and its implementation before reporting the results of the data analysis.

4.2 Questionnaire design

Following the initial design of the questionnaire, it was subject to extensive review and revision before being piloted. Piloting tested that the questionnaire was meaningful and understandable to the respondents and secondly, to assure that the resulting data would be suitable for analysis. Interviews with a sub-set of the pilot group took place to further assure the appropriateness of the questionnaire and to get meaningful respondent feedback. Finally modifications were made to the questionnaire (see Appendix 5) before it was formally distributed to the research sample. The research sample was drawn from the whole of the UK. The postal questionnaires were sent to the Systems Development Manager at each organisation.
with an accompanying letter outlining the purpose of the research (see Appendix 6) whilst the electronic distribution was accompanied by an email that sought to do the same (see Appendix 7).

4.3 Sampling

The questionnaire was sent to:

1. A DP mail list which includes IS professionals.
2. Ninety alumni of De Montfort University postgraduate computing programmes.
3. Ninety large and small companies all of whom claim to provide a complete systems development service. Companies were selected paying due regard to their size, role and geographical location.

The DP mail list is managed by the Joint Information Systems Committee and is an arena within which DP and IS issues are frequently presented and discussed. It is regarded, therefore, as a suitable source of information regarding the views of both IS personnel and DPOs in the areas of IS and DP.

The introductory section on the questionnaire clearly stated that the questionnaire is to be completed by those with experience in information systems development. Over eighty percent of responses were from people with a "strong" IS job title thereby adding strength to the view that the results are representative of the IS profession. It was not possible to sort responses into the original three mailing categories; this is regrettable in that significant insights may have been forthcoming.

Fifty nine usable responses were received and before considering the data (see Appendices 8 and 9) it is worth providing a brief summary of the demographic profile of respondents. The questionnaire included a section that collected data regarding the nature of the respondent group. This was done to allow for an assessment of

---

9 Commonly known as 'JISC', the Committee has organised many events and published widely in the field of IS and DP, and in particular on the implications of DP for higher education.

10 For example, those specified in section 2.2 as being at the core of the IS profession.
representativeness to occur and to facilitate analysis at an occupational level. The two largest groups represented in the respondent set are Project Managers and Managers/Directors of Information. These groups represent a significant proportion of respondents, accounting for almost half and this has implications regarding the finding of this research and for future research. The respondent group are an experienced body of IS professionals. Almost half of the respondents have worked in the IS profession for between one and five years whilst most of the rest have been in the profession for more than six years. The majority of these staff will have been in an IS position within organisations during the period when the 1998 DPA was enacted and implemented.

Two thirds of responses came from personnel working in large (more than 1000 employees) organisations. Only one fifth of respondents worked in organisations with less than 100 employees and it may be that personnel working in smaller companies may have a very different view of PDP. With regard to economic sector represented in the study the following respondent profile emerged:

<table>
<thead>
<tr>
<th>Economic Sector</th>
<th>No of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Enterprise: Computing</td>
<td>18</td>
</tr>
<tr>
<td>Public Sector</td>
<td>13</td>
</tr>
<tr>
<td>Private Enterprise: Non-Computing</td>
<td>12</td>
</tr>
<tr>
<td>Academic</td>
<td>9</td>
</tr>
<tr>
<td>Self Employer/Contractors</td>
<td>3</td>
</tr>
<tr>
<td>Other</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 4.1: Economic sector and respondent analysis

Sample design sought to target sufficient respondents to allow for a representative sample to emerge. Actual respondents are experienced IS professionals that are representative of the IS profession, in a wide range of organisations of different sizes. It is suggested that the profile presented allows for valid judgements to be made and presented.
4.4 Questionnaire results and data analysis

The research found considerable support for the involvement of IS personnel in the provision for PDP. The vast majority of respondents believe that:

- IS personnel have a significant contribution to make in assisting organisations meet their PDP obligations.
- PDP is a legitimate activity for IS personnel to be involved with.
- PDP is an increasing concern for IS professionals.

For many IS professionals the provision for PDP is a major part of their professional life. IS personnel are active in determining and implementing the PDP policies within organisations. It was reported that in one third of organisations IS personnel have primary responsibility for PDP and in one quarter PDP is a shared responsibility between IS personnel and DP personnel within their organisations. More than half of respondents report that in their organisations IS staff are involved in formulating and implementing DP policies for all staff.

These findings confirm the view that IS personnel have an important role to play in the provision for and management of PDP and that this role is seen as legitimate by members of the profession.

4.4.1 Which IS personnel and what activities present PDP enhancing opportunities?

The role of IS personnel in the provision for PDP is a relatively recent development and it may be a consequence of this that the precise nature of that role is presented in a general rather than specific manner. This research sought to discover 'which IS personnel and what IS activities present PDP opportunities?'.
9. In your view which three information systems jobs/roles provide the greatest opportunities to enhance privacy and data protection within information systems?

10. In your view which three stages in your systems development life cycle provide the greatest opportunities to enhance privacy and data protection within information systems?

Table 4.2 presents the responses to the first of these two questions:

<table>
<thead>
<tr>
<th>IS Role (identified by &gt; one respondent)</th>
<th>Number of respondents identifying role¹¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT/MIS/Systems Manager</td>
<td>28</td>
</tr>
<tr>
<td>Systems Analyst</td>
<td>19</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>12</td>
</tr>
<tr>
<td>Systems Developers</td>
<td>11</td>
</tr>
<tr>
<td>Systems Designer</td>
<td>9</td>
</tr>
<tr>
<td>Systems Administrators</td>
<td>7</td>
</tr>
<tr>
<td>Project Manager</td>
<td>7</td>
</tr>
<tr>
<td>Network Manager</td>
<td>6</td>
</tr>
<tr>
<td>Programmers</td>
<td>6</td>
</tr>
<tr>
<td>IT Security Personnel</td>
<td>6</td>
</tr>
<tr>
<td>Data Protection Officer</td>
<td>5</td>
</tr>
<tr>
<td>Support and Training</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 4.2: IS roles in the provision for PDP

A notable feature of the data presented is the identification of managers as key providers in the provision for PDP. Some respondents felt so strongly about this they annotated their response with emphasis on role of senior management. In the literature review the role of managers in facilitating PDP within the IS profession and within systems was not prominent. It may be that the emphasis on PETs and systems design may lead to a neglect of the important role of management in the provision for PDP. The role of systems designer is not as significant in the data as one may expect given the prominence they have in the literature. This may be a consequence of terminology because if we take ‘systems developers’ as being synonymous with ‘systems designer’ then the role becomes much more prominent. However, at this stage the data supports the conclusion that the staff

¹¹ These numbers represent the frequency with which a particular role was stated by respondents.
identified in this study as having the greatest opportunity to support PDP are
Project Managers, Systems Analysts and Systems Designers/Developers. Given
this insight we can now turn our attention to a consideration of which stages in the
IS development process offer PDP enhancing opportunities.

Stages in the systems development process that were identified by respondents in this
study as offering opportunities for PDP are shown in table 4.3:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Number of respondents identifying stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Design</td>
<td>35</td>
</tr>
<tr>
<td>Systems Analysis</td>
<td>21</td>
</tr>
<tr>
<td>Implementation</td>
<td>17</td>
</tr>
<tr>
<td>Project Initiation and early planning</td>
<td>13</td>
</tr>
<tr>
<td>Testing</td>
<td>10</td>
</tr>
<tr>
<td>Training users</td>
<td>5</td>
</tr>
<tr>
<td>Embed in the whole process</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 4.3: Stages in the systems development lifecycle that offer opportunities for PDP enhancements

Systems analysis and design are identified as being the areas in which the greatest
contribution can be made. It is worthy of note that systems design is the most
frequently stated stage whilst in the roles identified it does not feature as prominently.
This is further evidence to support the view expressed earlier that respondents are
using the term 'systems developer' to describe someone who undertaking systems
design. Looking at the individual responses for those that state 'design' as a stage it is
interesting to note that eight of them include 'developer' and not 'designer' as a role.
This would suggest that they are linking the developer role to the design stage.

It is interesting to note that five respondents suggested 'embed in the whole process',
or 'all stages' rather than identifying three individual stages as requested in response
to question ten. This unprompted response suggests that respondents feel strongly
that PDP awareness and practice should be present in all aspects of IS development
work. As a result of this finding the data was further analysed to see if there were any
respondent characteristics that provide additional insights into this outcome. Those
reporting this 'all stages' type of response were from different occupational
categories, i.e. one Manager/Director of IS, a Database Administrator, a Project
Manager and two Systems Analysts. All but one work in organisations with more than 1000 employees and three of them also identify Managers of IT/IS as being key staff in the provision for PDP. At first sight it was thought that these respondents may be seeing a ‘bigger picture’ than other respondents, but upon further data analysis it became apparent that the way the data was being analysed was perhaps problematic. The response to question ten consists of up to three ‘stages’ which were aggregated with all other responses to this question and analyses at the aggregate level and therefore in isolation of their context. Looking at the data in context added significant meaning. The analysis of the data at the level of each response showed that seventeen other respondents presented their three stages in a life cycle sequence, i.e. analysis, design and implementation. This may mean that many more respondents than were first thought are suggesting life-cycle coverage with regard to opportunities for embedding PDP into systems development.

Evidence has been presented that shows that IS personnel have an important role to play in the provision for PDP and this section shows which IS roles can contribute most and in what stages. We now go on to consider whether IS personnel are equipped to meet the challenge.

4.4.2 Are IS personnel equipped to meet the challenge?

Identifying IS personnel as instrumental in providing systems that facilitate PDP means that it is crucial that this group are aware of both the framework and their responsibilities within it. We have seen how at a national level IS personnel have been identified as critical to the implementation of PDP within organisations and within information systems. Most IS personnel that contributed to this research accept that responsibility and can identify particular roles and opportunities for contributing to PDP. This section considers whether the profession is ready to meet these challenges and, if not, what needs to be done to better support IS personnel in meeting the challenges they readily accept.

A starting point for this analysis concerns levels of awareness with regard to PDP and the legislative framework within which it sits. A simple question to address
is, ‘how aware are IS personnel of PDP issues?’ Levels of PDP awareness amongst the respondent group were reported as high. A high proportion report that they know how the principles found in the 1998 DPA affect the development of IS and an equally high number report that they are aware of how the DP principles affect the operation of information systems. It may be that this high level of awareness is a reflection of the composition of the respondent group rather than a broader reflection of awareness in the IS hinterland. Those that responded may simply be the IS personnel that are actively involved in provision for PDP and as such they may be more knowledgeable than their colleagues. This issue will be examined further during the case study research that followed this survey.

Looking at the IS profession as a whole, 30% felt that ‘awareness of the 1998 DPA amongst IS staff is high’, whereas 51% felt that it was not. These findings are similar to those found in the IMIS ‘Survey into Professional Practice’ (Prior, 2003, p36) which shows that 30% felt that awareness of DP amongst IS personnel is high whilst 46% felt that it is not. Respondent characteristics and their individual responses to this particular question are examined in an attempt to identify any correlations that may inform these findings. For example, 62% of responses came from personnel in organisations that have more than 1000 employees. It may be that awareness in companies such as this is higher than the industry standard due to formal training opportunities that may exist more in larger organisations than smaller ones. It may also be that what is being reported here is a management view of levels of awareness rather than the view from a broader body of IS personnel. Completing a questionnaire on PDP may appeal more to ‘privacy advocates and/or privacy professional’ than to other IS personnel that may feel exposed by a lack of awareness or uncertainty with regard to PDP. Further research using the case study approach explored this in more detail and is reported in the next chapter.

If IS personnel are to design compliance into computer systems then they need to be operating in a context that is sensitive to, and supportive of, PDP. Clearly, designing a compliant system will be less effective if it is used in an organisation that does not provide a supportive environment and culture for PDP. It was found in the survey that 80% of respondents work in companies that have a general PDP policy for all
staff. This appears a positive context for the development of systems that are compliant with PDP requirements. However, responses to the statement ‘I have a detailed knowledge of my organisations [privacy and data protection] policy for all employees’ are reported in table 4.4:

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>5%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disagree</td>
<td>20%</td>
</tr>
<tr>
<td>Indifferent</td>
<td>20%</td>
</tr>
<tr>
<td>Agree</td>
<td>27%</td>
</tr>
<tr>
<td>Strongly agree</td>
<td>27%</td>
</tr>
</tbody>
</table>

**Table 4.4: Awareness of PDP policies**

More than half feel that they have a detailed knowledge of their PDP policies, however, the extent to which PDP policies are understood by other staff in organisations are reported as being much lower. However, just over one third report that, in their view, company polices are not understood or applied by their colleagues. If stated policies are not known or applied then this may undermine even the most privacy sensitive computer systems or procedures. DP is as much about human systems as computer systems; PETs and effective systems design can assist in safeguarding against human failings but it cannot guarantee protection.

Based on the evidence presented here, awareness for those that are active in the field of PDP is reported as being of an acceptable level but awareness amongst their IS colleagues is regarded as considerably lower. Awareness is an issue that can be significantly affected by training and other awareness raising events, and given this, the survey sought information regarding training and support offered in the area of PDP. Only four respondents agreed with the statement ‘organisations are providing suitable training in PDP issues for employees’. Thirty two disagreed with the statement whilst thirteen were ‘indifferent’. Ambivalence with regard to support being offered by professional bodies was also reported. Seventeen respondents felt that appropriate guidance was provided, twenty nine were indifferent whilst thirteen felt that appropriate guidance was not provided.

A major finding of this survey is that managers have a critical role to play in the provision for PDP and given that they are seen as so important their data was subject
to further detailed analysis. Twenty seven responses were from individuals with the word 'manager' in their job titles and this sub-set of data showed the following:

1. Fourteen 'strongly agreed' that IS staff have a significant contribution to make to PDP. Eleven more agreed with the view, whilst one was indifferent and one disagreed.

2. Only eight managers feel that awareness of the 1998 DPA is high.

3. Confidence is high amongst this group with regard to how the DP principles affect IS development. Twenty five of them reported that they are aware of the implications.

4. Not a single respondent felt that organisations are providing appropriate training in PDP.

5. Only two members of this group were involved in the consultation process that accompanied the development and implementation of the 1998 DPA, with a lack of awareness of the opportunity to contribute stated as the main reason for not contributing.

6. Regarding DP policies, seven managers report that they feel these policies are understood by employees with eight reporting that they feel they are being applied.

This important group in the provision for PDP present themselves as knowledgeable and prepared to contribute. They present data that can be used to question whether organisations are providing the context for effective DP provision and, in particular, within the IS development process.

The survey data presented here supports the following conclusions:

- Some IS personnel are prepared to support PDP through their professional practice.
- IS personnel can and have identified which staff can contribute to PDP and at what stage in the SDLC.
- IS and business managers have a fundamental role to fulfil in creating an environment in which PDP practices are understood and applied.
Current levels of awareness of PDP issues amongst the general body of IS personnel may be at a level that will not support them in meeting the objectives set by the IC of becoming a key player in developing privacy enabling systems. The age of the 'ethical engineer' is perhaps not yet with us.

Overall management strategy and commitment is as important as technical or procedural design factors.

Training and further professional guidance is required at an industry wide level.

4.5 Contribution to theory and refining research questions

Evidence has been presented showing that this new role responsibility is accepted by some members of the IS profession. Indeed, the evidence presented would suggest that IS personnel positively support their involvement in safeguarding privacy and data. From this positive position it is possible to identify some factors that may need to be addressed for organisations to fully benefit from this support being offered by members of the IS profession. Paramount amongst these is the role of senior managers in creating organisational cultures and business practices that are fully supportive of PDP. Organisations cannot provide PDP through systems design, PETs and IS professional practice alone; the management context and wider organisational culture within which data is processed is, and always will be, critical to the provision of PDP.

It was always intended that the analysis of the questionnaire data would feed into the refinement of the case study design and as such it is appropriate to outline the main aims of the next stage of this research:

- Seek greater input from systems or business analysts, systems designers and programmers.
- Undertake case study research with a small number of organisations to explore with IS personnel the contribution that they feel they can make in the provision for PDP and how this impacts on IS practice.
Chapter 5: Case Study - Role of DP and IS personnel in the provision for PDP

5.1 Research questions and methodological issues

The previous chapter concluded by supporting the view that IS personnel are increasingly identified by government agencies and their representatives as critical to the successful implementation of PDP legislation. Survey evidence has been presented showing that this new responsibility is accepted by some members of the IS profession. Indeed, the evidence suggests that some IS personnel positively support their involvement in safeguarding privacy and data. However, it is possible to identify some factors that may need to be addressed in order for organisations to fully benefit from the support being offered by members of the IS profession. Paramount amongst these is the role of senior managers in creating organisational cultures and business practices that support PDP. Organisations cannot provide PDP through systems design, PETs and IS professional practice alone; the management context, organisational culture within which data is processed, and the views of business managers, IS managers, and IS personnel are critical to the provision of PDP. Before considering how this affects the proposed research it is necessary to examine two features of the respondent profile.

A large number of respondents in the survey were ‘managers’ in ‘large organisations’. Almost half of respondents had the word ‘manager’ in their job title and more than two thirds were from organisations with more than 500 employees. This profile may mean that the survey and its conclusions are representative of a partial view of the IS profession and its practices. The survey showed a high degree of acceptance for PDP responsibilities and a high level of PDP awareness amongst respondents; further work needs to be undertaken to assess the extent that this is truly reflective of IS personnel. This gives rise to a reformulation of the research questions and objectives. The original research questions were:
1. What is the role of IS personnel in the provision for PDP within systems and organisations and how aware and accepting are they of their obligations?

2. What aspects of IS professional practice have PDP enhancing opportunities and how widely known or applied are these?

The emphasis on management and context that emerged during the survey research means that an additional research question is being added at this stage, which is:

3. What is the role of IS management in the provision for PDP and how does that interface with other DP managers in organisations?

In seeking to explore these related research questions it is intended to gain deeper insights into the IS development process than the survey achieved. In particular, the research will seek to gain the views of systems or business analysts, systems designers and developers. These are the groups that previous research identified as having the greatest contribution to make in providing for PDP and this case study research will examine this finding further.

Before presenting the analysis of the case study data several important methodological questions regarding this case study research need to be considered. These questions include:

1. What type of case study is this research?
2. Will the research study a single case or multiple cases?
3. Will the case(s) be from one or more industry sectors?
4. How will the case(s) be selected?
5. What impact will these decisions have on the robustness and generalisability of findings?

In seeking to answer these questions an outline of Yin’s threefold classification of case study types is presented and considered (Yin, 1993, p5). This is followed by a review of the literature concerning single or multiple cases. The decision whether to study one or more cases in this research is then made and justified. This is followed
by a review of candidate industrial sectors that may provide a suitable context for the research; again a decision is made and justified. This section then concludes by reviewing guidelines for selecting case(s) and considers the impact that the decisions taken will have on the robustness and generalisability of findings.

Yin (1993, p5) suggests that case studies can be classified as exploratory, descriptive or explanatory and which type a case study is, depends on the nature of the questions asked. Exploratory case studies are undertaken before the formulation of theory. Indeed, the prime purpose of an exploratory case study may be to assist in the identification or clarification of theory. Descriptive case studies allow for a detailed description of phenomena to be produced. Explanatory case studies seek explanations for given situations and/or causal relationships between phenomena.

This case study research uses features of both descriptive and explanatory case study designs. Yin suggests that research focusing on ‘how’ and ‘why’ questions may be best supported by the adoption of a descriptive study design. This research is seeking to discover and describe ‘how’ IS personnel contribute to the provision of PDP in organisations and ‘why’ they do it in the way that they do. The emphasis on ‘how’ and ‘why’ in this research supports the adoption of a descriptive case study design. This research results in detailed descriptions and analysis of professional practice in the provision of PDP, providing new insights into current IS practice in the provision for PDP. In this respect the research exhibits features of the explanatory case study type described by Yin.

With regard to using single or multiple cases Yin (2003, p39) presents a further classification of case study designs and outlines the circumstances in which each could be used. A brief review of these four designs provides a context in which an informed decision can be made regarding the design most suitable to support this research. The four designs Yin presents are:

1. Single case design with a single unit of analysis.
2. Single case design with multiple units of analysis.
3. Multiple case designs with a single unit of analysis in each case.
4. Multiple case designs with multiple units of analysis in each case.
In supporting single case study research Yin suggests that the research may be seeking to test a well-formulated theory in a ‘critical case’ that meets previously defined conditions to test the theory. Alternatively, the case may be a ‘unique case’, which, by definition, cannot be replicated and is therefore always a single case. The converse of this is the ‘representative case’ that is perceived to be typical of other cases in a particular population. The forth justification offered is the ‘revelatory case’ for which access is or has not been available by other means. The final justification of single-case study research Yin suggests is the ‘longitudinal case’ in which the single-case is studied over an extended period of time.

Yin (2003, p42) cautions that a ‘potential vulnerability of the single-case design is that a case may later turn out not to be the case it was thought at the outset’.

Regarding the search for ‘representative cases’, Ward-Schofield (2000, p78) adds that a single case, once found, may turn out to be ‘atypical in many important respects’. However, given the characteristics of some single case study research the choice of single or multiple cases simply does not arise.

Many authors (Yin, 2003; Walsham, 1995; Ward Schofield, 2000) support the view that multiple case studies are usually preferable to the use of a singe case study. This important issue will be considered further once the characteristics of multiple case study research are considered. Yin (2003, p46) suggests that multiple cases are appropriate for the study of innovation in organisations. If, for example, an innovation is adopted in many organisations, they can be studied as individual case studies, whilst the study as a whole covers many organisations. A major advantage of a multiple case strategy is that stronger evidence may result from the research. Yin states that the evidence resulting from multiple-cases is generally more compelling and has greater validity than that based on a single case. Ward-Schofield (2000, p79) states that multi-site studies increase the potential for generalisability of findings. In undertaking multiple case study research Yin (2003, p47) suggests that we are seeking ‘replication, not sampling logic’. In doing this we can select cases to seek either ‘literal replication’, in which we predict the same results from each case, or ‘theoretical replication’, in which we predict contrasting results for predictable reasons. Yin goes on to suggest that research involving between two and four cases is
usually seeking 'literal replication' whilst six to ten cases allows for 'theoretical replication'.

The discussion so far raises three important questions for this research. Firstly, will it involve the study of one or more cases, secondly, will it seek 'literal' or 'theoretical' replication and finally will the study address one or more unit of analysis within cases?

This research involves the study of three individual cases. The reasons for this are as follows:

1. Only one of the five justifications (a representative case) for single case study design that Yin presents is applicable to this research. However, the multiple case justification, 'the study of innovation in organisations' is wholly applicable to this research.
2. The use of multiple cases supports 'literal replication' that will provide 'more compelling evidence'.
3. Using multiple cases increases external validity.
4. Multiple cases are within the (limited) resource capabilities of this research.
5. Given the limited resources available for this research any increase in the number of cases would result in a reduction in the depth of analysis that could be undertaken within each case.

The focus of this research will primarily be on 'literal replication'. The use of three cases with a pre-determined degree of homogeneity and the descriptive nature of the research will provide the context for predicting similar results in all three cases. Moreover, the process of triangulating the findings provides 'literal replication' in that findings are expected to be similar for predicable reasons across all three cases. It is anticipated that this research will also allow for a degree of 'theoretical replication'. If two cases report or exhibit a set of conditions that are conducive to the provision of PDP and these are 'literally replicated' between the two cases then we can theorise that an absence of these conditions may lead to a situation in which the provision of PDP is less supported and less developed, and test that in the third case. In other words, we can predict contrasting results for predictable reasons.
The final question to answer from the discussion so far concerns the unit of analysis. This research will be designed to address two units of analysis within each of the three cases. The first unit of analysis concerns the role of IS development staff in providing PDP in the systems development process. The second unit of analysis concerns the management of PDP.

When deciding if the research will be conducted in one or more industry sectors two main issues were considered; firstly the degree to which the study seeks 'theoretical replication' and/or 'literal replication' and secondly the homogeneity of the case population and its impact on generalisability of findings. This study is seeking 'literal replication' and a rich understanding of particular phenomena and as such cases are required to be similar in their histories, structures and procedures, i.e. have a controlled degree of homogeneity. Yin's (2003, p51) consideration of using multiple cases to support theoretical replication is also relevant here. In support of theoretical replication Yin suggests that this strategy is appropriate if the 'realm of external validity' is complex. For this study the external environment is complex and it is theorised that different industry sectors have responded to the increasing need for PDP in a wide range of different ways. The reasons for these differences in presumed responses may include, amount of personal (especially sensitive) data handled, exposure to external pressure to conform to current legislation, awareness of PDP and accountability to external bodies.

Researching IS personnel in one industrial sector increases the potential for generalisation of findings to other cases in the same sector. IS personnel in the UK work in a broad range of settings, with different structures, processes and priorities and in this respect the profession lacks homogeneity. Selecting cases from different industrial sectors may mean that the specific and different influences on each sector's provision for PDP cannot be isolated from their context. If this were to be the case then this would seriously restrict the ability to undertake cross-case data analysis, to triangulate and to generalise findings. Using one industry sector for this research limits the research in that the findings will be more supportive of 'literal replication' rather than on 'theoretical replication' and the generalisability of findings will be primarily restricted to the one sector. However, it is argued that these are worthy outcomes in their own right. Whilst researching one industry sector is a more modest
strategy, the findings may, depending on the sector selected, be generalisable to a large part of the UK provision for PDP. Moreover, there will be opportunities for measured generalisation to theory concerning other industry sectors.

Walsham (1995) suggests that generalisations are possible by the ‘drawing of specific implications in particular domains of action’. This means discovering and describing the relationship between a given situation and its ‘generative mechanisms’ and applying these to other situations. Discovering ‘generative mechanisms’ within one industry sector may facilitate generalisability of these mechanisms within the sector. Given the discussion above, this research will focus on the provision for PDP within one industry sector.

The selection of one industry sector was undertaken in the following manner:

1. Examining the industrial profile that characterises the region this study is confined to, i.e. the central counties of England, and identified candidate industry sectors.\(^{12}\)
2. A list was compiled of criteria for inclusion in the study (see Appendix 10).
3. Each sector was then assessed to the extent to which they meet the criteria.
4. The sector with the highest score was selected.

The selection process outlined above resulted in UK Local Authorities (LAs) being selected as the industry sector for this research. This research will therefore focus on the role of IS personnel in supporting the provision for PDP within UK LAs. The final choice of LAs was not altogether surprising given that De Montfort University staff have strong links with LAs and because of this the decision to undertake this research within LAs may have been influenced by a presumption that access to staff in LAs may be easier to gain than in other industry sectors. How individual LAs were selected and the difficulties experienced in gaining access are dealt with in the next section.

\(^{12}\) This self-financed research was constrained in that no resources were available to cover the cost of undertaking the research over a wider geographical area.
Yin (2003, pp47-8) states that an ‘important step in all these replication procedures is the development of a rich theoretical framework’ and it is from this framework that generalisations to other cases become possible. The framework should state the conditions that support ‘literal replication’, i.e. the conditions under which phenomena is likely to be found and the conditions under which it is not, ‘theoretical replication’.

In considering how many cases is enough it is necessary to revisit the issue of theory in case study research because selecting cases is interwoven with case study theory. It is widely accepted that sampling logic should not be used in selecting cases (Yin, 2003; Walsham, 1995; Ward-Schofield, 2000). Yin (2003, p51) suggests considering the number of ‘case replications - both literal and theoretical - that you need or would like to have in your study’. Relevant to this study, he adds that ‘you may want to settle for two or three literal replications when rival theories are grossly different and the issue at hand does not demand an excessive degree of certainty’. If on the other hand cases have subtle differences and a high degree of certainty is sought then five or more replications may be appropriate. With regard to theoretical replication Yin (2003, p51) suggests that it is important to consider the complexity of the ‘realm of external validity’. If uncertainty exists about the external environment and its impact on case outcomes then a higher number of cases may be appropriate. These uncertainties should be articulated at commencement of the study. In this research the rival theories are yet to be developed and, at this time, a need for a high degree of certainty does not exist. This research is, therefore well supported by two or three literal replications.

Yin (2003, p47) highlights the importance of developing a rich theoretical framework that states conditions under which particular phenomena are likely to be found (literal replication) as well as conditions when it’s not likely to be found (theoretical replication). The theoretical framework becomes the vehicle through which generalisation to other cases can be made. As stated previously, this study will be supported by the selection of three cases to provide a context that allows for ‘literal replication’. The cases are expected to exhibit similar outcomes in relation to the evaluation theory. The study will focus on how and why particular outcomes are present and seek literal replication of these conditions from case to case. If similar outcomes are not revealed, the use of ‘triangulated’ cases could be expected to give
substantial clues about why they were not, and as an aid to further research in the field.

Gomm, Hammersley and Foster (2000, p 103) suggest two ways of generalising from a small number of cases, drawing ‘theoretical inferences’ and drawing ‘empirical generalisations’. Theoretical inferences refer to the process of identifying what always happens or what may happen with a given degree of probability in certain circumstances. If it is found in this research that PDP provision results from external pressures that are consistent over the sector we can suggest that what is found in these cases may also be found in other LAs; in other words, we can generalise. ‘Empirical generalisations’ refer to the process of drawing inferences about the features of a larger population of cases from the study of a sample drawn from that population. This is clearly the case in LA and PDP. Gomm et al, (2000, p 103) state that empirical generalisations means ‘reaching conclusions about the distribution of particular features within a population’. They explicitly acknowledge and agree with the contribution of Ward-Schofield in highlighting the importance of homogeneity of the population in allowing for this form of generalisability.

Silverman (2000, p 102) suggests that selecting a representative sample from a previously defined population is not usually available in qualitative research, adding that ‘very often a case will be chosen simply because it allows access’. He goes on to suggest that we consider the particular setting to be studied, the elements of process on which to focus and how the results might be generalised. Commenting on typicality of cases to support generalisation Ward-Schofield (2000, p 78) adds that ‘carried to extremes or taken too seriously the idea of choosing on the basis of typicality becomes impossible, even absurd’. However, she does support seeking typicality especially when combined with the production of ‘thick descriptions’. She adds that ‘thick descriptions provide the information necessary to make informed judgements about the degree and extent of the fit in particular cases of interest’. This study will not therefore be applying any formal sampling strategies in the selection of case study organisations. However, the selection of LA as a context for the research has highlighted that similar features exist within organisations in this sector.
In selecting cases Yin (2003, p78) suggests screening case study nominations according to a defined set of ‘operational criteria whereby candidates will be deemed qualified to serve as cases’. If this process results in a large number of eligible cases Yin suggests undertaking further fact finding about the cases and defining further qualifying criteria to screen and reduce the eligible number to between twenty and thirty. Finally, randomly select the number of cases required from final twenty to thirty. As we shall see later (see section 5.2.1) the luxury of having more cases than needed and selecting between them was not an option available in this research.

Before considering the robustness of findings and their generalisability it is worth summarising the main decisions that have been taken so far:

- According to the Yin classification this research is a descriptive case study that will result in the production of ‘thick descriptions’ of phenomena.
- The research will also exhibit features of the explanatory case study in that the research will provide explanations for the patterns of PDP found and its relationship to its context.
- The research will focus on three case study organisations with two units of analysis in each case.
- One industry sector is chosen, i.e. Local Authorities in the Midland region of the UK.
- Replication logic rather than sampling logic will drive the selection of case study organisations for inclusion in the study.
- Three case study organisations will take part in the research.

It is suggested that the choices presented above represent a rational and appropriate framework for supporting this research. The production of a thorough case study protocol (see Appendix 4) evidences the extensive attention to design that has been employed in this research. This attention to detail and design will increase both external and internal validity of the research and the homogeneity of the case context will contribute to the robustness of findings and their generalisability.
5.2 Preparation for the case study research

5.2.1 Finding cases

Finding cases prepared to participate in this research was extremely difficult and time consuming. Finding potential cases for this research involved a review of the ‘The Computer User Year Book’ (2003). All local authorities in three central UK counties were identified. From these, a case study selection criteria was applied, i.e. number of IS personnel, which reduced the list to seventeen potential cases. Letters (see Appendix 11) were sent to the Head of IT and the Data Protection Controller in each of these seventeen LAs. These letters were accompanied by a Frequently Asked Questions sheet (see Appendix 12) concerning the research and a Consent Form (Appendix 3). This initial contact was followed-up by a telephone call a few days later and in most case many more calls over the following days and weeks until three consenting organisations were found.

The difficulty experienced in persuading LAs to participate in this research cannot be overstated and as this is methodologically significant it is worthy of further consideration. Only one of the three case study LAs (LA2) was a ‘willing’ participant; they immediately agreed to participate in the research. LA1 became a participant following some gentle encouragement by the lead researcher. This gentle encouragement took the form of providing assurance that the views of personnel working in smaller LAs were as valid and important to the research as those of personnel in larger LAs. The third and final case study organisation proved the most difficult to recruit. Whilst data collection was underway in LA1 and LA2 the search for a third LA to participate continued. A record of contacts with each LA (telephone calls, letters, messages left, etc) was maintained and managed with a view to positively encouraging participation. After many weeks of telephone calls and letters most LAs had either refused to participate or it had become impossible to actually speak to the person within LAs who could make the decision to participate or not. The IT Manager in LA3 was finally persuaded to participate following the application of gentle pressure by a personal friend of the lead researcher who happened to be working in LA3.
Methodologically it should be noted that any initial reluctance to participate was not something known to respondents within the LAs and as such it does not adversely affect the views recorded in this study. The personal contact in LA3 did not contribute to the research and respondents were not aware of our association. The difficulty experienced in gaining participants to this research is a lesson that will not be forgotten.

5.2.2 Piloting research instruments

At the same time as the process of finding cases was being undertaken the piloting of research instruments was also underway. Senior DP and IS personnel at Bradford Metropolitan District Council agreed to pilot the research instruments. Document review and interviews were conducted which allowed for the interview questions to be tested out on a range of staff, including the Senior Policy Officer (Governance), Head of ICT, Head of Information Services and two member their IS development staff. The results of these interviews were then analysed and the research instruments updated. The piloting also allowed the researcher to discover issues about their own interviewing style and effectiveness and these were recorded contemporaneously for subsequent analysis and action. It was decided that the interviewing style used at the pilot stage would be replaced by a more conversational style of dialogue in the actual research interviews. Piloting therefore resulted in:

1. Confirmation that the questions and discussion points were appropriate and meaningful to respondents.
2. Assurance that the data forthcoming was pertinent to the research.
3. A modification of the interaction style from an interview to a less structured discussion.
4. The development of supplementary materials to illustrate points and to assure a consistent context for respondents to consider questions. Examples of these include the list of DP principles and a notional systems development lifecycle given as visual prompts during the research.
5.3 Data analysis strategy and procedures

The case study design and data analysis considerations that have been outlined in this chapter and in sections 3.2.4 and 3.4 led to the development of a specific data analysis plan that was applied to the case study data. The process of data analysis is guided by the principles and procedures of grounded theory and as such the development of analysis codes was undertaken as follows:

Step 1. Restate the research questions.
Step 2. Restate the theoretical propositions.
Step 3. Identify from analysis of 1 and 2 an initial set of categories and codes.
Step 4. Read the data and code according to the initial set of codes (open-coding) and identify emerging (new) themes and codes.
Step 5. Segment the data to facilitate data analysis within categories whilst allowing for the identification of new themes and codes and the relationships between them, i.e. axial coding.
Step 6. Aggregate the findings of step 5 into overall findings/conclusions.

The results of each step are presented in table 5.1:

<table>
<thead>
<tr>
<th>Step 1. Restate the research questions</th>
<th>Step 2. Restate the theoretical propositions (reflecting the original research objectives)</th>
<th>Step 3. Identify from analysis of 1 and 2 an initial set of research codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RQ1: What is the role of IS personnel in the provision for PDP within systems and organisations and how aware and accepting are they of their obligations?</td>
<td>1. There is a commitment amongst IS personnel to protect data and to provide data privacy. 2. Organisations face similar challenges in responding to DP regardless of their size and complexity. 3. Levels of awareness may be less than that required to effectively respond to the DP challenges. 4. Rapid changes in the legislative context may inhibit commitment to DP. 5. Levels of commitment</td>
<td>RL Role  BG Background  TR Training  LEG Legitimacy  AW Awareness  EF Effectiveness of DP in ISD and Organisation  IMP Improvement strategies  MAN How DP is managed  LC Lifecycle stages and PDP  ISS IS personnel and their contribution  SD Systems development  SDC Systems development</td>
</tr>
</tbody>
</table>

RQ2: What aspects of IS professional practice have PDP enhancing opportunities and how widely known or applied are these?
RQ3: What is the role of IS management in the provision for PDP and how does that interface with other DP managers in organisations. The role may vary in a consistent manner at different occupational levels.  

6. More can be done to embed PDP practices in the systems development process.

SD/DP Systems Development with a DP emphasis PR Principles

---

**Table 5.1: Stages in the development of data analysis codes**

<table>
<thead>
<tr>
<th>Step 4. Read the data and code according to the initial set of codes and identify emerging (new) themes and codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The transcripts of the eleven respondents in three cases were read and coded according to the categories identified in step 3. This gave insights into a range of emerging themes that are coded as follows:</td>
</tr>
<tr>
<td>OD</td>
</tr>
<tr>
<td>DS</td>
</tr>
<tr>
<td>S</td>
</tr>
<tr>
<td>EUC</td>
</tr>
<tr>
<td>LI</td>
</tr>
<tr>
<td>SR</td>
</tr>
<tr>
<td>RM</td>
</tr>
<tr>
<td>CP</td>
</tr>
<tr>
<td>ICM</td>
</tr>
<tr>
<td>DA</td>
</tr>
<tr>
<td>CUL</td>
</tr>
<tr>
<td>EG</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5. Segment the data to facilitate data analysis within categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>The data analysis carried out in step 4 highlighted the need to segment the data for further, more focused analysis. The existing sequentially structured data (in order of data collection) was then restructured in the following way:</td>
</tr>
<tr>
<td>1. By occupational category, i.e. Data Protection Officers, IT Managers and Systems Developers.</td>
</tr>
<tr>
<td>2. In question of the initial set of interview questions within occupational categories.</td>
</tr>
<tr>
<td>3. According the pre and emerging codes.</td>
</tr>
</tbody>
</table>

Once restructured in this way the segmented data was then reanalysed and the findings recorded before step 5 commenced.

<table>
<thead>
<tr>
<th>Step 6. Aggregate the findings of step 5 into overall findings/conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>This outcome of this step is to identify and report findings that transcend more than one segment of the data. The findings are reported later in this thesis.</td>
</tr>
</tbody>
</table>

The data analysis procedure that was followed in preparing data for analysis included:
- Separating interview transcripts into occupational categories of Data Protection Officers (DPO), IT Managers (ITM) Development Team Leaders (DTL) and Developers (D).
- Coding all interview transcripts in interview question, research code and occupational role order.
- Aggregating the data according to respondent role and research code. This involved the grouping together of previously separate coded categories into new aggregated data analysis categories as outlined in the next section.
- Data analysis was undertaken using horizontal and vertical analysis of data. Horizontal analysis consists of reviewing the same cluster of data analysis categories across all four occupational roles being considered whilst vertical analysis considered how each occupational group felt about individual codes within their clusters.

Once data was sorted into these categories certain issues emerged that needed to be considered prior to further data analysis, these include:

- Certain occupational groups were more concerned with particular issues than other groups. This was anticipated and is reflected in the revision of the data analysis codes outlined in the next section.
- New codes emerged as important to participants and these are reflected in the revised data analysis codes.
- One DTL was concerned about a number of issues that were not mentioned as significant by his peers or his managers.

These initial data analysis findings and the discovery that some research codes that appeared prominent in the literature were less prominent in these cases supports the revision of the data analysis codes and procedures. Similarly, initial data analysis uncovered a tendency on behalf of respondents to deal with or comment on several codes together. Some identified codes rose in prominence during data analysis, such as Security, whilst others, such as risk management, current priorities, E-Government and inconsistent messages from government appeared less significant than first anticipated. This led to the aggregation of codes into new data analysis categories and
The new aggregated categories used to structure and focus the data analysis are presented in table 5.2:

<table>
<thead>
<tr>
<th>Aggregated Data analysis categories</th>
<th>Original research codes in new data analysis categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background and context of DP in organisations</td>
<td>Role, Background and Training</td>
</tr>
<tr>
<td>DP management</td>
<td>How DP is managed, Ownership of data, Data sharing, End user computing, Liaison between data people, Shared responsibility, Data audits, Culture</td>
</tr>
<tr>
<td>Evaluation of DP provision in organisations and information systems development.</td>
<td>Awareness, Effectiveness of DP in ISD and organisations, Improvement strategies</td>
</tr>
<tr>
<td>Information systems development and DP</td>
<td>Legitimacy, Life cycle stages and PDP, IS personnel and their contribution, Systems development, Systems development changes, Systems development with a DP emphasis, DP Principles</td>
</tr>
<tr>
<td>Security</td>
<td>Security</td>
</tr>
</tbody>
</table>

**Table 5.2: Data analysis categories resulting from initial data analysis**

It became apparent during the interviews and during early data analysis that the category of staff in LA two that represented Developers were actually DTLs with considerable responsibilities for the management of systems development. During the interview process it was made clear to these respondents that the views being sought from them were those of the developers they represent and not the views of managers. As such they were invited to respond to questions in the light of their personal experiences as a developer and as a representative of their development teams. At the time this was seen as a reasonable compromise to overcome the obstacles that existed in gaining access to actual development staff, however during initial data analysis it became apparent that many of the views being expressed were more managerial and supervisory than developmental. It was decided that this insight could be used to enhance the research by the introduction of a new occupational grouping between
ITMs and Developers; this analysis category is known as DTLs. The resulting occupational roles used for data analysis were:

<table>
<thead>
<tr>
<th>Role</th>
<th>Number of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LA 1</td>
</tr>
<tr>
<td>Data Protection Officer</td>
<td>1</td>
</tr>
<tr>
<td>IT Manager</td>
<td>1</td>
</tr>
<tr>
<td>Development Team Leader</td>
<td>-</td>
</tr>
<tr>
<td>Developer</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 5.3: Occupational roles for data analysis

Before going on to review the finding under these new data analysis categories it is necessary to provide a brief outline of the organisational context.

5.4 Case study description and justification

Three local authorities (referred to as LA1, LA2 and LA3 for the purpose of this discussion) contributed to this research.

1. LA1 is a rural authority in a market town serving a population of approximately 75,000 and covering approximately 230 square miles. Seven permanent staff and a separate E-Government team support the IT function. The IT function draws upon consultants for specialist and extra support at times of particular need. The IS Manager/DP Officer and a Senior Developer contributed to this research.

2. LA2 is a County Council serving a large population located in a mixture of county towns and villages. The authority has a knowledgeable, dedicated and active DPO (with the job title ‘Compliance and Records Manager’) and a ‘centrally managed locally delivered’ IT function. The IT function is led by the Applications Development Manager (referred to in this study as an ITM) has approximately 63 full-time equivalent staff. They are located in four major departments of the authority providing IT services and support. The IT function with each department is managed by a DTL who reports to the ITM of LA2. The ITM and DTLs manage the work of development staff, project managers, systems analysts and business consultants. The ITM, DPO and four DTLs contributed to this research.

3. LA3 is a Unitary Authority serving a large town and its surrounding district which in itself contains a further six small to medium towns. DP within this authority is
managed through the work of a DP Officer who is a member of the IT team. The IT function is supported by four full-time retained staff, the ITM, the DP Officer, a Freedom of Information Project Worker and an E-Government Project worker. Apart from these roles the IT function has been outsourced to an IT services provider as part of a Public-Private Partnership. Many of the IT staff that worked for the authority now work for this IT services provider. The ITM, the DP Officer and two developers contributed to this research.\(^{13}\)

The structural and procedural complexity of DP and IS provision within these LAs was an expected feature of their work. LAs are highly accountable to their elected members, central government and the public they serve. These IS personnel, therefore, have to respond swiftly and positively to a range of initiatives and pressures from an equally wide range of sources. At the time this research was undertaken the priority for many IS personnel was to meet the FOI compliance deadline which, at that time was only a few months away. It was frequently stated that DP had been put to one side to allow resources to be focused on FOI issues. The other major development current at the time of this research concerns the Children’s Act of 2004 (OPSI, 2004) which gave considerable responsibilities to LAs for the management and coordination of children’s data, services and protection. The data storage and data sharing aspects of this Act were being watched with considerable interest by the ITMs involved in this research. Respondents in this research regard themselves as under pressure to deal with current and rapidly changing pressures and DP was not, at the time, seen as one of those.

The justification for selecting Local Authorities is outlined in section 5.1 of this thesis and it is worth noting at this stage that the research process confirmed the rationale of the case study selection criteria. These organisations are all heavy users of data, they are committed to effective data management and DP procedures and as such if DP

\(^{13}\) Interviews with the two developers in LA3 were conducted with both respondents at the same time. Methodologically this is significant for a number of reasons. Firstly, the interview questions were designed to be answered by individuals on their own, but by allowing for a group interview to take place the views expressed by both participants may be different to that which may have been expressed had they been alone. It is a recognised feature of focus group research that respondents may feel a loss of privacy in group situations and there is a danger of ‘over-disclosure’. Both of these may affect the validity and reliability of the views expressed. (Morgan, 1998, p90)
awareness, commitment and maturity are to be found anywhere, these are likely candidates.

5.5 Case study: Analysis and findings

5.5.1 Role and background of respondents

Having provided some insights into the organisational context of this study it is now necessary to provide some background information of the respondents that contributed to the research. The initial interview questions focused on gathering background information on respondents and their organisations and their role in relation to PDP. Information was also sought regarding the experiences and training respondents have had in the area of PDP. It was felt necessary to establish the credentials of respondents so that their comments and views could be considered in a more informed way.

All organisations have a designated DPO, albeit with different titles. In LA1 the DPO role is undertaken by the ITM, in LA2 the DPO is called the Compliance and Records Manager, reflecting a role that is broader than DP alone. His role is to assure DP at an operational level and DP policy making at a strategic level. The DPO in LA3 describes his role as ensuring legal compliance, liaison and advisory within the whole area of DP.

The DPOs in this study have considerable experience in the field of DP. The DPO in LA1 has had 7-8 years specific responsibility for DP, whilst the DPO in LA2 has been involved with DP since the 1984 DPA. The DPO in LA3 claims more than 20 years experience in both DP and IS Project Management. In all three organisations DP has close historical links with IT. In LA1 the DP responsibility is performed by the ITM, in LA2 the responsibility for DP used to be in the IT Department until the appointment of the DPO in 2004. The DPO in LA3 was in the past a senior member of their IT Department before the IT function was outsourced. This close relationship is significant for this research because it is interested in understanding the relationship between staff involved in the provision for DP and in examining the influence DP is
having on IS practice. Because current DP provision is either in, or was until recently in, the IT function means that IT staff should be aware of any increasing pressure on them since the passing of the 1998 Act to embed DP into systems and the systems development process.

The size and internal organisation of the DP and IT functions in the three organisations differ. LA1 is the smallest of the case study organisations and within it DP and IT are managed by the same person who is supported by a Senior Developer (referred to in this study as LA1 D1). The DPO/ITM is responsible for DP throughout the organisation and its systems. LA2 has the largest in-house IT function with an ITM who devolves the delivery of IT services within service departments to distinct teams that are led by a DTL. These DTLs describe their role as managing development teams. LA2 ITM specifically states that his role is to try to ensure that as many of the eight DP principles are known and applied by his staff and, whilst acknowledging that this is primarily done on trust, it is nevertheless interesting to note the early reference to the eight principles of the 1998 Act. IT and DP are managed differently in LA3 from the other organisations in this study. IT services are provided by a Public/Private Partnership (PPP) arrangement. This recent development has resulted in many IT personnel who were employed by the authority being employed by the PPP company that now provides IT services. This means that although the provision of IT services is now outsourced, it is outsourced to many of the same staff that previously provided these services in-house. As such there exists both continuity and opportunities for close liaison between retained staff and those now working for the PPP company. This means that the views expressed by D1 and D2 in LA3 can be regarded as sufficiently representative of the case study organisation.

DTL and developers are involved in all stages of the systems development process. Three of the DTL describe their role as ‘managing a development team’, whilst the fourth describes his role as a ‘Senior Project Manager’. In LA1 the Senior Developer adds the terms ‘Data/Systems Analyst’ to describe his role adding that he is responsible for all stages of the development life cycle. In LA3 the Business Analyst (D1) liaises with users to produce a specification of the proposed system which is then handed to developers to implement. D1 and D2 in LA3 are a formally recognised team working together developing systems for service departments in the authority.
The DPOs and ITMs in all organisations report that training and support in the area of DP is forthcoming. Induction and ongoing web-based training features in all three organisations. The DPO in LA1 provides training and support directly through personal contacts and via a range of intranet initiatives. The services of external organisations are used to deliver specific DP training. DTLs report that training in LA2 is provided at induction and as part of their management training programme. In LA3 over 600 staff have been trained in DP issues during the period 2001-5 which is further supported by the purchase and implementation of new web-based training materials.

The views of the DPOs and ITMs are supported by their staff. In LA2 DTL1 reports that he has recently attended two or three courses in the area of security. DTL3 recalled his DP training at both induction and as part of his management training programme whilst DTL4 confirms his use of the web-based training materials. In LA1 the Senior Developer works closely with the DPO/ITM and as such he is very close to the development of the DP framework and the production of DP policy documents. He is clearly aware of DP issues and supports the DPO/ITM in raising awareness throughout the organisation. In LA3 D1 reports that he had received a half day training 3 years earlier that focused on Subject Access Request procedures. His colleague, D2, reported that he had undergone some general DP training which, he added, 'had nothing to do with IS development'. Indeed this respondent went on to express his belief that 'we need to decide whose responsibility DP is before deciding if more training is needed'. This issue became more prominent as the research continued and is considered in more detail later in the next section of this thesis.

5.5.2 Management of DP

The original research questions focused on the role of IS staff in the provision for PDP and in doing so it emerged that the role of IS management was perceived as increasingly important. This led to the identification of a third research question that this research would address and it is to a consideration of this question we now turn. The following areas of DP management are considered:
How DP is managed?

Ownership of data and data sharing.

DPOs and ITMs in all organisations were able to outline the structure and processes involved in the delivery and management of DP. In LA1 the management of DP can be described as personal, with structural clarity. The DPO/ITM works personally with the Heads of service departments and reports that all service Heads are committed to effective DP. In LA2 and LA3 the management of DP is more complex and in both organisations important uncertainties emerged. In both LA2 and LA3 DP is managed at a corporate level by the DPO who has DP representatives working in the service departments to whom local DP issues should be addressed and if necessary the local DP representative can elevate an issue to the DPO if it cannot be resolved at a department level. In LA2 DTLs in service departments channel their DP concerns either through the service area DP representative or through their own IT line management structure for onward transmission to the DPO. The DPO confirms that he receives queries from both the service department and IT routes. It was reported in LA2 that IT and the DPO are beginning to explore ways of bringing the DPO into their development processes to strengthen DP within systems and processes and this is considered further in section 7.6. In LA3 the DPO role is to liaise with the PPP company with regard to developing systems specifications. It was reported that DP is formally considered as part of these specifications. This process was known to staff and appears to be used effectively.

The IT Manager in LA2 describes his role within the context of uncertainty with regard to DP responsibility, which is a recurring theme. Whist accepting some responsibility for DP he adds that ultimately it is the user departments that are responsible for DP. In LA3 the DPO and ITM are both positioned strategically within the organisation, sitting as they do on high level strategic management committees. Representation at this level assures that DP is supported and has a high profile.

DTL1 in LA2 highlighted the devolution of DP responsibility pointing out that all DP related decisions cannot be passed to the DPO. Developers must make judgements
and if they miss something then it is hoped that the Senior Developers will identify the issue and deal with it. DTL and developers are aware of the role played in service departments by the DP Liaison Officers and the conduit they offer in seeking guidance on DP issues. Indeed, this process is frequently cited as working well from many sources within the organisation and as such it is accepted as effective. Moreover DTLs also report that their developers feed DP questions to and through them to the DPO and he uses both ICT and the user department DP Liaison Officers to feedback information regarding new legislation and procedures. The developers in LA3 report that it is their view that DP is the responsibility of the user department managers.

The literature review found considerable evidence to support the view that DP is increasingly an IS responsibility. The questionnaire data supported this view and its analysis concluded that whilst IS responsibility is well documented and accepted there was a lack of clarity with regard to what that role actually is and these case studies sought insights into this unknown issue (Howley, 2002). With regard to the management of DP in these organisations it is clear that the data is the responsibility of the user department and the role of IS personnel remains unclear and is at best, advisory. This is clearly at variance to the finding of the literature review and survey. The ITM in LA2 states that IT and end users have a shared responsibility for data but the ‘end users have the right to do what they want’. DTLs in the same organisation support and share their manager’s view pointing out that ‘responsibility for data is shared but the client is the data owner’. DTL4 adds that he doesn’t feel that his staff should constrain the users, rather they should advise when asked, but ultimately it’s their data. Developers in LA3 echo this sentiment. The question of whose data and who is responsible will re-emerge in this discussion as an important topic offering insights into the provision of DP in organisations and the role of personnel in the matrix. However, the discussion about where responsibility for DP lies is particularly interesting in relation to increasing data sharing between organisations.\(^{14}\)

\(^{14}\) The challenge of data sharing is an issue that can be informed by developments in Privacy Theory. James Moor’s (1997) ‘Control Restricted Access Theory of Privacy’ and Roger Clarke’s (2006) concept of ‘Information Privacy’ provide a useable theoretical context within which the privacy concerns that data sharing brings about can be explored.
Several recent cases evidence both the increasing need to share data and the uncertainty and nervousness that surrounds this practice. During the period 2000-2004 we have witnessed the Victoria Climbie (Laming, 2003), British Gas (BBC, 2003) and Soham (BBC, 2004) cases all of which resulted in a loss of life and a subsequent attempt to ‘blame’ DP legislation for restricting the officials concerned in the extent they can share data about people at risk or who are themselves a risk to others. These cases and the corresponding attempts to ‘blame’ DP legislation served to both elevate DP into the public consciousness and highlight the claimed complexity of modern DP and the increasing amount of data sharing (DS). DS is a feature of modern business processes and the three organisations in this study are involved in schemes to facilitate DS. Major concerns were expressed regarding the Children’s Act of 2004 (OPSI, 2004) which will require and regulate data sharing across a range of social, health and public services. DS is high on the agenda in LAs, NHS Trusts and other public bodies with the DPO in LA3 pointing out that the pressure to share data experienced a set-back at the time of the Soham case but is now firmly back on the agenda in the form of ‘controlled DS’. The ITM/DPO in LA1 reports the main DS concern as one of how to share sensibly and remain legally complaint. These intra-organisational sharing issues are a concern of ITM, DPO and DTL, but at the developer level the concerns are more about inter-organisational DS.

Developers fully support the managerial view that data and DP is the responsibility of users and their managers. DTL1 in LA2 puts it clearly and bluntly, ‘it’s their information and they are responsible for it, not ICT’, adding that in their view it is the information owner and not ICT that is responsible for PDP. They acknowledge that developers, as part of determining requirements, have a responsibility to find out how they want to manage their information and what safeguards they want to put on that information. They add that if the users ‘are doing it wrong’ the developer has a responsibility to say so especially when working with non-senior users. As they put it ‘it not passing responsibility over to them, its sharing responsibility, but ultimately the decision is theirs .... as it is with all other businesses’. DTL3 adds, ‘we are ICT services, but there is no DP responsibility within my team other than in a general way ...... we have a highly defined standing that the data belongs to the service department and not to us’. Both developers in LA3 suggest that the ‘customer should drive DP; it’s their responsibility’. However, in response to a question ‘would customers be
grateful if you flagged-up a DP issue?’, they pointed out that customers would expect them to highlight DP issues adding that they think it’s part of our general work responsibility and that ‘responsibility needs to reside somewhere’.

DTL1 in LA2 suggests that they work closely with customers but cannot impose a system on them, ‘it’s their information and they are responsible for it ... if we saw a problem [it’s] our professional duty to say so, but that’s it. It’s their data and processes, even if we automate it’. DTL3 in LA2 refers to the term a ‘general responsibility’ when referring to his staff and DP and again restates the conventional wisdom that it is the user departments that are responsible.

Clearly the responsibility for DP is recognised as an issue that IS personnel have to consider and to which they can contribute, but the IS personnel in these case study organisations are clear and united in their view that DP is the responsibility of the user department and their management. The role of IS personnel in these organisations in the provision for DP is advisory and secondary.

5.5.3 Evaluation of effectiveness of PDP

It follows on from the earlier research that awareness of DP is an issue in that if IS personnel are not aware of DP in a general manner or how they could contribute to it specifically then their contribution would be restricted (Howley, 2002). ‘Awareness’ is a critical code in this study and it is to a consideration of this that we now turn.

LA3 DPO describes DP awareness as ‘indifferent, not good, not bad’ pointing out that a considerable amount of training and support has been and is provided. Evidence to support the extensive provision of training and guidance was forthcoming in all three LAs. Online training and supporting documents were reviewed by the lead researcher and as such the question of their effective use is inevitably raised. LA1 ITM pointed out that there were ‘pockets of lack of awareness’ but his data professionals are more aware. He describes DP training as considerable and provided in part due to a fear of being ‘caught out’. DTL1 suggests that awareness is at its highest amongst public-facing and partnership-linking staff and senior developers. He also points out that
awareness of DP is a response to data sensitivity in that, in his area, DP is not considered often, whilst in other areas he believes that it will have a much higher profile, offering Social Services as an example. He adds that, personally, he feels vulnerable regarding his DP knowledge and suggests that the organisation needs to do more to raise awareness. DTL2 claims that all his Project Managers, Systems Analysts and Business Analysts are aware of DP but that they focus more on data integrity and data security. DTL3 reports that his staff would probably recognise DP principles but DTL4 believes that his staff would recognise them from their background as data professionals rather than as part of the 1998 DP Act. He adds that the principles are not at the forefront of their working day but they do feel a general responsibility for them. When prompted about sensitive data he acknowledged that his staff are aware that their data is ‘sensitive’ at a general level but, he adds, they would not be aware of the technical meaning of sensitive data as defined within the 1998 Act.

In LA1 D1 suggests that DP guidelines are known and used more at a management level than at a user level, adding that ICT staff are well aware of DP. The Business Analyst (D1) in LA3 claimed that he was not confident regarding DP but feels that he has an appreciation level of awareness whilst his colleague D2 is less clear and relies on D1. This shows that whilst the literature and questionnaire data supports the view that IS personnel are increasingly responsible and that they have a contribution to make, staff ‘on-the-ground’ feel exposed and ill-prepared to fully contribute. This finding supports the research reported earlier in this thesis which showed that many IS personnel are ill-equipped to contribute to the extent suggested in the literature review.

With regard to effectiveness of DP provision within organisations, varying responses were forthcoming. LA3 DPO describes it as ‘medium’ acknowledging that a lot more could be done but time resources restrict it. LA3 ITM believes that DP in ISD is good even though two of his development staff regard DP as a ‘pain in the neck’ (see section 5.5.5.1 for further consideration of this ‘telling’ comment). The ITM in LA1 claims that there has been a lot of discussion about data management and security, but not DP in ISD, and had nothing to suggest regarding improving DP in his organisation. The ITM in LA2 acknowledges some ‘weaknesses’ and that ‘odd errors
do creep in’ but he concludes that ‘mostly DP is effectively provided for’. In LA3 the ITM states that DP provision ‘is good .... it's engrained in the work we do and part of good IS practice’. Commenting on both general DP and DP in ISD in LA2, DTLs 1 and 2 use the term ‘reasonable’ whilst DTL3 uses the term ‘adequate’ pointing out the possibility of elevating an issue up to the DPO. DTL4 is stronger when referring to his team of developers using the term ‘very effective’ adding again that for data it’s the users’ responsibility and that he cannot comment on that. Developers’ views range from ‘good’ in LA1 to ‘sometimes DP is not even considered ... the profile of DP is not high’ in LA3.

In evaluating DP in these organisations it become clear that:

- Staff at more than one level lack confidence in DP.
- DP awareness is still regarded as low or at best ‘patchy’.
- DP requirements are not yet embedded into the ISD process.
- Commitment to DP is higher at managerial levels than at developer levels.

Given these observations and the increasing and positive acknowledgement by these respondents of the need to consider PDP it is reasonable to seek insights into how these IS personnel feel that the provision for PDP can be improved.

5.5.4 Improvement strategies

It was always intended to seek the developers’ views of what they feel can be done to enhance DP provision within ISD and in organisations generally and this section reports on responses under this code. DPOs suggest that DP needs a higher profile in authorities, pointing out that, in their view, positioning the DPO in the organisation is crucial to successful DP. LA1 ITM reports that he has to limit improvement plans to avoid alienating service departments. DTL1 in LA2 is currently reviewing improvement strategies with his ITM. More general suggestions included:

- DP should be built into the original businesses requirements and into design.
• A clear set of guidelines are needed regarding the levels of protection systems require and to apply them consistently.
• Standardise Developer roles and job responsibilities with regard to DP.
• Publicise and raise awareness of who does what and who’s responsible for what and then enforce it.
• A developer suggests that a refresher course on DP would be welcome.
• A developer from LA3 suggested defining processes and a list of initial questions [highlighting DP issues] that IT services can give to users prior to any project start up.
• The other LA3 developer agreed and suggested publicising a policy regarding storing of data and disclosing public information.
• LA3 D1 proposes formalising DP as part of ISD to avoid it being a consequence of individual knowledge or commitment.

It is perhaps interesting to note that developers have more suggestions to make than ITM or DTLs perhaps suggesting that there is perhaps more demand (or need) for DP guidance than there is leadership.

5.5.5 Information Systems Development

This research area is concerned with the impact of PDP on ISD and in exploring these issues the following research codes are considered:

a. Whether PDP is a legitimate concern of IS personnel.
b. Stages in the SDLC in which IS personnel can make significant contribution.
c. What contribution IS personnel can make to PDP.
d. Changes in the process of ISD as a result of PDP.
e. Relationship between ISD and the DP principles.

5.5.5.1 Whether PDP is a legitimate concern of IS personnel

The research sought the views of IS personnel with regard to the extent to which DP is legitimately their responsibility. LA1 ITM feels that his IT staff realise the
importance of DP. LA3 ITM feels that DP is a legitimate concern of his, adding that 'I cannot duck the responsibility as part of the Information Management Group'.

LA2 DTL1 suggests that DP is a concern of his staff but only 'in partnership with customers .... Senior Developers, Business Analysts, etc., yes, it's their job .... less so junior techies .... good staff would agree it's their responsibility'. DTL2 feels that DP is a legitimate concern of his and his Business Analysts, especially if DP is the same thing as security. He feels that his Developers would see DP as integrity of data. DTL3 feels that his staff have 'a general responsibility to DP .... but it [DP] is a very legitimate concern of IT'. LA1 D1 regards DP as a relevant concern of IT staff and adds that the more you concentrate on it at source, the better. He goes on to add 'it's no good trying to apply security to a system after it's been developed'. In LA3 some contradiction of views were noted in that D2 feels that developers should flag DP issues to management for them to deal with, adding that a DP framework is needed to guide developers. His colleague, D1, adds, 'Yes. I am responsible, but DP is a pain in the neck'. Both agree enthusiastically with this final comment pointing out that in their view DP is not considered much by developers. Their DPO believes that 'that most staff do DP without realising it'; a view not stated by his colleagues.

Frequently it was reported that DP is a legitimate concern of the IS professional because 'we are data professionals and as such we care for data'. It was also reported that 'we deal with data responsibly, because we are responsible people'. This may be an example of IS personnel responding to new challenges by locating them within their existing framework of professional expectations and practice rather than seeking to develop, and therefore accept, a broadening of their role. At management level there is a total acceptance of DP as a legitimate concern of IS personnel but amongst developers different opinions surfaced. When a developer in LA3 stated that DP was a 'pain in the neck' it was enthusiastically supported and enjoyed by his colleague. When asked 'if data security is a pain in the neck' he responded immediately, 'No. It's a pain in the neck if we don't deal with it'. 'Data Protection', for this respondent was not highly valued, but 'Protecting Data' is. This may provide a fundamental insight into the perceived value of externally imposed responsibilities on the IS role, i.e. the need to accommodate DP, compared with the higher value that may be placed on an internal and professionally developed response.
to a new responsibility or a broadening of the IS role, i.e. increasing the protection of data.

5.5.5.2 Stages in the ISD life cycle in which IS can make significant contribution

If results show that IS personnel can contribute and it is a legitimate concern of theirs, then it is reasonable to seek insights into just what form that contribution can take. This refers back to the questionnaire findings that showed systems analysis and systems design were the most cited stages. This study sought to develop these findings further and as such respondents were asked to identify the stages in which IS personnel can make the greatest contribution to PDP in ISD. The DPO in LA2 immediately referred to the contribution being made throughout the whole lifecycle, with an emphasis on the initial business case specification and the Project Initiation Document. The DPO in LA3 also identified the Project Initiation Document, adding Feasibility Study, design and testing as the main stages. The IT manager in LA1 responded to the question by suggesting that ‘security is built in from square-one ... with an emphasis on security throughout’. This substitution of the term DP with security was noted with interest and led the researcher to pose the question, ‘so security would be DP?’ The answer to which was, ‘yes, by and large’. There was an increasing and strong trend to answer questions about DP, as if DP and security are synonymous. LA3 ITM stated that up-front activities are very important as is project management and testing. When prompted by the researcher about design’s prominence in the literature he agreed that design is important adding that all stages are significant. DTL4 points out that DP should be dealt with early in the life cycle adding that you can’t retrofit protection. He suggests that we should get users to fully understand the DP implications of their processes and data. Again he suggests that DP should be considered early, i.e. ‘when going through the initial gathering of what the project has to do .... the start and testing they’re the pressure points’. The Developer in LA1 states that DP is discussed as soon as IT becomes involved in projects adding that users consider it in their requirements specification. At LA3 D1 went straight for design whereas D2 identified the business study stage as the most significant adding that this is where the data and accesses are defined. D1, prompted by his colleague’s contribution, also adds the Feasibility Study stage as important.
5.5.5.3 What contribution can IS personnel make to PDP?

Related to the stages and again building on the earlier survey work this study sought insights into which staff can make the greatest contribution and the results of this are shown in table 5.4:

<table>
<thead>
<tr>
<th>Research Respondent</th>
<th>1st role identified</th>
<th>2nd role identified</th>
<th>3rd role identified</th>
<th>Other comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>LA1 ITM</td>
<td>Designer</td>
<td>Systems Analyst (SA) / Business Analyst (BA)</td>
<td>Programmers and testers</td>
<td>Adds operators and technical staff to assure that principle seven is catered for. When prompted about Project Managers he suggested they would be involved checking all aspects.</td>
</tr>
<tr>
<td>LA3 ITM</td>
<td>Project Manager</td>
<td>Designer</td>
<td>Developer</td>
<td>Links to stages identified.</td>
</tr>
<tr>
<td>LA2 DTL2</td>
<td>BA</td>
<td>Project Manager</td>
<td>Developer</td>
<td></td>
</tr>
<tr>
<td>LA2 DTL3</td>
<td>SA</td>
<td>Designer</td>
<td>-</td>
<td>This respondent links DP to decision making that takes place early in development and adds that decisions are not made by those later down the life cycle who code from a specification. Questions such as, ‘why you want data’, ‘what you do with it’ and ‘how do we get rid of it all’ are seen as critical DP questions.</td>
</tr>
<tr>
<td>LA2 DTL4</td>
<td>Project Manager</td>
<td>SA</td>
<td>Developer</td>
<td></td>
</tr>
<tr>
<td>LA1 D1</td>
<td>BA</td>
<td>SA</td>
<td>Whole team</td>
<td>Discussion went on to identify the SA as most important</td>
</tr>
<tr>
<td>LA3 D1</td>
<td>BA</td>
<td>Developer</td>
<td>BA is the official job title of this respondent and his colleague LA3 D2 is a developer.</td>
<td></td>
</tr>
</tbody>
</table>

Table 5.4: IS personnel with the greatest contribution to make

These findings support the survey findings in that systems analysts, business analysts and developers feature strongly as they did in the survey data. Project managers are also identified as having a contribution to make by two respondents. Overall these
findings support the conclusions arrived at earlier in this research in that the significant staff in leveraging PDP into the development process are those that are involved early in the process, Analysts and Project Managers.

5.5.5.4 Changes in the process of ISD as a result of PDP

This section sought insights into how the process of ISD has or could change in the context of an increasing need to consider PDP and the following comments were forthcoming:

- Greater focus on questions such as, ‘why you want data’, ‘what you do with it’ and ‘how do we get rid of it’?
- When using outside contractors get them to sign-off forms and letters assuring that they have provided DP compliance.
- Use DP checkpoints to force all stakeholders to focus on key DP issues at key stages in development process.
- Include a DP peer review process.
- A policy for DP in ISD needed.
- Include DP in project mandate and charge it back to customer.
- Increasing use of anonymising strategies for publicly available data.

Respondents were asked to focus on how ISD takes place with an emphasis on DP. DTL3 says that attitudes have changed and a great deal is happening in the data management world, DP, FOI, interoperability standards, E-Government, etc, have all profoundly affected attitudes to ISD and whether to buy in or develop systems in-house. In LA1 the implication of DP has led to many small databases being removed and more centralised and controlled data management. LA1 ITM confirms that DP and security are included as part of the detailed systems proposals and are carried forward into systems specifications. The DTL1 in LA2 claims that his team doesn’t explicitly consider DP but he would welcome a clear set of guidelines on what level and type of protection are suitable for particular types of systems that would ‘stop the need to reinvent the wheel every time a new web system was being developed’. DTL2 refers to how his team have increasingly been designing for security and DP over recent years. DTL3 refers to the Applications Development Policy which provides
guidelines for developments adding that more guidelines are needed and in particular we need to make more people aware. DTL4 is not aware of any specific DP steps or processes to 'add' DP, 'it's almost in the fabric of what we do'. He goes on to add 'I think if I put my hand on my heart there isn't a lot that we consciously say 'this is a DP ... issue'. It's almost a mute acceptance that we are going to be careful, but there are no explicit DP reference points that you link to during an applications development.'

5.5.5.5 Relationship between ISD and the DP principles

With regard to UK DP principles there was a strong focus on principle seven (the application of appropriate technical means to secure data). This was not surprising, but the overwhelming enthusiasm for participants to recast their DP responsibilities in 'Security' terms was. Many respondents sought to talk about security claiming that it is synonymous with DP. A Development Team Leader in organisation two explained 'when I say security what I'm talking about is privacy and data protection ... I think the two things go hand in hand'. D1 in LA1 responded to the question 'Is DP a legitimate concern of yours?' with the answer is 'I think it's relevant because the more you can concentrate on these things at source the better. There is no good trying to apply security to the system after it's been developed. If we control security of data it means the DP task is a lot easier'. This comment supports the view that supporting DP in systems development should come early in the life cycle and secondly shows the single-minded focus of this developer on security. The question posed was about 'legitimacy' not 'security'. This developer immediately and without hesitation substituted 'DP' with 'security' again showing the tendency to contextualise DP within a security framework.

When prompted most respondents could and did give examples of how their work can, and does, support all the principles and this confirms the survey findings which concluded that IS personnel have a role encompassing the whole life cycle and supporting all DP principles. However, unprompted responses to the question, 'Which principles can IS personnel best support?' usually led to the immediate identification of principle seven followed by principles concerned with volume of data, use to which data is put, retention periods and data quality, i.e. accuracy and integrity. The overwhelming view of many respondents is that DP is synonymous with security, whilst the view of the author is that it is much broader than that.
DTL2 states that ‘if staff don’t know how to realise principle seven then they are not much use ... and principle four ... accuracy’. He goes on to add that they may monitor principle three, (adequate and not excessive) which he adds may become an issue but ‘if it looked OK we wouldn’t necessarily raise it’. When prompted to continue with this thread of discussion he added that if it looked excessive it would be up to the BA to decide how to respond. Regarding collecting information that is ‘excessive or not’ it’s the BA that would deal with that and they would do so in the interests of efficiency rather than according to the requirements of the 1998 Act. LA2 DTL3 suggests that principle seven is the first one to focus on but adds that ‘we don’t really focus on any particular principles – government reporting requirements are more important drivers of what data we store’. We support principles from ‘an osmosis point of view, we are data professionals, but ... no... I don’t believe my development staff could deal with too many of these’. D2 in LA3 states that ‘principles and DP issues are covered in training but we aren’t lawyers – we can only apply basic principles ... so need to keep it simple’. Are these ‘data professionals’ seeking to define DP responsibility as a legal issue rather than an IS development one, and if they are, is this a legitimate course of action? The two comments from D2 in LA3, ‘we aren’t lawyers’ and ‘we can only apply basic principles’, may be specific attempts to redefine or relocate DP responsibility away from IS personnel and onto others in the complex DP arena.

5.5.5.6 Security

Throughout this study it has been difficult to focus answers to DP questions away from a singular focus on security. IS personnel have an acute sensitivity to data security; it’s bred into the very fabric of their professional responsibilities and as such this topic emerged as worthy of review. The DPO in LA2 reports that, ‘data protection and information security come as one’. DTL1 stated that ‘when I say security what I am talking about is privacy and data protection’. DTL2 adds that ‘systems integrity would be discussed and systems integrity includes security and these may well include a consideration of DP. My job is part of systems integrity; it is not my job to implement the Data Protection Act; it’s my job to know something about
it and to ensure it’s one of the considerations’. DTL3 answers a plain, ‘Yes’ to the question ‘does DP equal security?’. LA3 D1 adds that ‘security is not DP; security is protecting the system and data is part of that, but DP doesn’t come up during the development process’.

The emphasis on security is interesting on a number of fronts. Firstly, it can be seen as a reasonable and appropriate response to increasing (and uncertain) privacy and DP requirements. Data professionals have always been the guardians of data and as such internalising or interpreting DP requirements in terms of ‘security’ provides a familiar context within which IS personnel can formulate their response to DP requirements. In this respect this is an effective and positive response to DP legislation and increasing privacy awareness. However, a slightly less desirable consequence of this emphasis may be that it allows those involved to avoid formulating an IS response to other requirements in the DP principles. Almost all respondents had to be prompted to consider principles beyond principle seven when considering their contribution to DP in systems development. This emphasis on security may artificially limit their contribution. Once prompted and provided with examples of how IS personnel can contribute more widely, respondents were enthusiastic about these suggestions. Discussions at this time led to the identification of a number of ways that IS personnel can contribute more effectively and these are considered in the next chapter.

5.6 Overall case study findings

This case study research has addressed three research questions and a range of theoretical propositions in the area of PDP and IS development and it is appropriate to summarise the main findings.

1. All three organisations in this study have defined structures and procedures for the management and delivery of DP. In all three organisations there exists a parallel framework for managing DP in that the IS function has a pathway, as do service departments within the LA. In the two largest authorities tensions in the delivery of DP were reported.
2. Whilst accepting a responsibility for PDP the IS personnel in this study see it as a collaborative endeavour between the IS personnel, DPOs and user departments, but the balance of responsibility remains unclear. Indeed, it is frequently reported by IS personnel that DP is the responsibility of the user department and not IT. The role of IS personnel in the provision for PDP is at best seen as advisory, personal marginal, and avoidable. At the other extreme DP was reported as being a ‘pain in the neck’ by one developer.

3. E-Government and DS are pressures that have increased awareness of DP issues in these authorities, but at the same time they add pressure on IS personnel to move their attention away from DP to enable them to respond to the most recent government priority in the data world.

4. Levels of awareness regarding DP are variable with public-facing personnel and those handling personal data regarded as being more aware than other staff. It was also noted that managers report greater confidence regarding DP in general, and DP within ISD in particular, than do others. Indeed, it was reported in section 5.5.3 that ‘staff on the ground feel exposed and ill prepared to fully contribute’ to DP.

5. None of the authorities had taken any steps towards changing their ISD practice in the light of the increasing PDP agenda. This is clearly at variance to the wishes of the IC.

6. DP Improvements strategies focused on defining roles and achieving clarity as to who is responsible and for what in the provision of PDP.

7. It was frequently reported that DP should be considered as early as possible during a systems development life cycle, but there was no evidence of this being the case amongst these LAs. This finding confirms the literature review conclusion that the role of IS personnel in the provision for PDP remains aspirational rather than actual.

8. The IS personnel identified as having the greatest contribution to make are those that are involved early and/or throughout the development process, Project Managers, Business Analysts, Designers and Developers being the most frequently identified roles.

9. A range of suggestions were forthcoming regarding how the process of ISD can change to support the aim of creating privacy sensitive systems.
10. In exploring the relationship between IS personnel and the 1998 DPA principles, responses usually focus on principle seven which concerns the need to apply appropriate technical measures to protect data. These IS personnel regard DP as the application of security to systems and data and were reluctant or unable to go beyond that.

These conclusions are supported by the PDP literature. Before the 1998 DPA came into force the multiplicity of actors involved and the complexity that brings about was predicted by Rabb (1999), Lycett and Pouloudi (1999) and France (2000). They all suggested that effective PDP requires a collaborative approach from all those involved in the provision for PDP. This research found no evidence of collaboration in this respect. As suggested in point two above there remains considerable uncertainty regarding relative responsibilities for PDP. Levels of PDP awareness amongst these case study respondents supports the data found within the literature (IC, 2001; IC 2006). Awareness of PDP is general and aspirational rather than specific and operational. Despite the work undertaken by, or sponsored by, the IC with regard to the application of PETs and ethical design (HiSPEC, 2002; OIC, 2006) there is no evidence of these aspirations becoming a reality at this time, despite the emphasis on security reported in this research. The importance of managers in the provision for PDP noted in point eight above is supported by the work of Lederman (2003). Lederman provides an interesting and potentially rewarding review of the relationship between data quality, as a privacy enhancing feature, and assesses the impact of this on the ISD process and the personnel within it.

5.7 Case study conclusions

This case study research provides valuable insights into how these three organisations are interpreting and responding to the PDP challenges they face. Their contribution to this research gives detailed insights into both the systems they develop and work with, and the procedures within which they conduct their working lives. It also gives a detailed insight into what they think and feel about the changes and challenges that increasing data related legislation brings their way.
Having reviewed the case study data and suggested some clear conclusions it is now appropriate to examine the findings from the case study research in conjunction with the survey data to provide an overall picture of how IS personnel in UK organisations are responding to the PDP challenge.
Chapter 6: Analysis and synthesis: Survey and case study findings

So far the findings of the survey and case study research have been presented separately and it is now appropriate to examine the findings in relation to each other. Before doing this, however, it will be useful to reflect on the data analysis strategy that was employed in creating the data these findings are based on. In doing this the conclusions will have greater validity.

6.1 Data analysis strategy revisited

The data analysis strategy for both questionnaire and case study data was reviewed extensively in section 3.6 of this thesis and as such it is not necessary at this stage to repeat the strategy in detail; a brief summary will suffice so that we can then review the effectiveness of the strategy. The theoretical framework for data analysis was that of grounded theory and content analysis.

The procedure of data analysis followed the steps outlined in section 3.6.2 and involved verifying the data, cleaning it, the production of ‘top-line’ data, cross tabulation, bivariate and multivariate analysis. This process was effective in identifying significant data for analysis and allowed for the re-examination of specific data sets that emerged as potentially significant such as the data concerning systems designers and the role of managers in the provision for PDP. The questionnaire data was analysed from different views, with different reasons, and inline with some of the principles of grounded theory.

The case study data analysis relied heavily on content analysis as the main theoretical and procedural framework. As outlined in section 5.3 the development of codes and their ongoing refinement in the analysis process proved very effective in structuring the analysis of a vast amount of textual data. The data was sorted in a variety of ways to facilitate analysis including by research codes, interview questions and occupational roles.
6.2 Findings: Research questions, objectives and theoretical propositions

The following section reviews each research question in the light of the evidence presented from the survey and from the case study.

6.2.1 Question 1: What is the role of IS personnel in the provision for PDP within systems and organisations and how aware and accepting are they of their obligations?

It has emerged that there is a very close relationship between IS personnel and the provision for PDP. IS staff are frequently the key personnel in organisations responsible for DP. IS staff accept their involvement in PDP as a legitimate and increasing concern. When the roles of IS and DP personnel are separate there exists a close relationship between the two and it was frequently reported that DP staff were in the past members of the IS group in their organisations. In LA2 IS and DP staff are starting to discuss strategies for the greater involvement of DP personnel in the ISD process.

IS personnel are reported in both the survey and in the case study organisations as being willing to accept a responsibility for DP. In the survey there was overwhelming support with 92% of respondents agreeing that IS personnel have a significant contribution to make to PDP and that this contribution is legitimate. Case study respondents agreed that they had a contribution to make but were insistent that their contribution was in support of others whom had the primary responsibility for PDP.

The case study research found that that the support for PDP, that appeared almost total in the survey, quickly became less forthcoming in the face-to-face discussions that took place. Development staff and their managers in this study readily accept responsibilities in the complex arena in which DP is provided for. In the case study organisations they see their role primarily in terms of applying security to their users’ data. The emphasis is very much on “the users’ data” and “the users’ system”. Indeed, the role of IS personnel is ‘vague’ and ‘hands-off’.

152
There exists a close relationship between IS and DP personnel with an acknowledged shared responsibility and fundamental desire to provide secure data. DP has emerged out of IS, and as such, the relationship and opportunities for future collaborations does exist. In two of the LAs there are plans to explore the way in which IS and DP staff can work together more effectively. In LA3 developers were keen to see the development of some DP ‘checks’ that can be applied during development processes. Whilst the ITM and DTLs in LA2 are looking to see at what stages the DPO can be involved in developments to apply a formal DP audit process on developments.

Both the survey and the case study research confirmed the belief that PDP is best realised when due attention is given to the early stages of a systems development life cycle and the roles that best support that are those of Project Manager, Business/Systems Analyst and Systems Designers/Developers. These are the roles that were seen has having the greatest contribution to make, but staff in those roles in this research were far from willing to be held responsible for PDP. Indeed, it was frequently reported by case study personnel that they had little or no awareness of any responsibility to build PDP compliance into systems and their associated procedures. This is a clear and significant tension.

Another shared finding is that Managers have a greater responsibility than other IS personnel; there is a hierarchy of DP. The most important role from the survey was that of Managers and in the case study it was found that developers were keen to rely on their more senior colleagues for PDP leadership. This is significant, not only in that there is presumed division of responsibility between IS personnel, but also in that it shows a lack of willingness to accept responsibility for DP amongst some staff. This is clearly at variance to the support that appears to be forthcoming with regard to legitimacy and the recognition that it’s an important part of the IS professional responsibility.

This research question is concerned not only with what is the role of IS personnel but how aware are they of that role. The findings of the case study research are that IS personnel are not aware of their role responsibilities and even if they were, their awareness of DP principles and how they relate to systems development and operation is at best thin and therefore quite unlikely to support the effective discharge of a
responsibility to PDP. Beyond ‘security’ there is a paucity of ideas about the application of privacy sensitive design during the ISD process.

6.2.2 Question 2: What aspects of IS professional practice have PDP enhancing opportunities and how widely known or applied are these?

The research has shown that the main IS development staff identified as being able to contribute to PDP are Project Managers, Systems Designers and Systems Analysts. Both survey and case study data shows that early intervention, and an ongoing concern for PDP, is the most likely way to assure compliance. However, both sets of data support the view that awareness of PDP is a barrier to effective delivery of PDP. This was a finding of the literature review and the subsequent research supports this finding.

Project management, systems analysis and design are seen as the most important stages and activities within which IS staff can contribute to PDP. In assessing what can be done within those stages the level of detail reduces as one probes more deeply. It is evident in this study that respondents had not considered PDP significantly in determining their systems development approach. Research firmly establishes the roles and stages but not what staff actually do within those stages. There is little beyond “applying security” with regard to embedding PDP in the SD process.

6.2.3 Question 3: What is the role of IS management in the provision for PDP and how does that interface with other DP managers in organisations?

One of the major findings of this research is the critical role of IS Management in the provision for PDP. They were the major group responding to the survey and taking part in the case study interviews and discussions. They were identified in the survey as the most significant group in creating a PDP sensitive IS development environment. Their role was identified as spanning the whole development lifecycle in terms of supporting the development of PDP sensitive systems. In the literature the focus with regard to PDP is on systems design and the application of PETs, however, this research has shown that this ‘low level’ focus may lead to a neglect of other
avenues that could be considered as offering opportunities for PDP enhancements. We may be seeking low level technical solutions to high level business problems.

IS managers have a responsibility for DP that spans the whole process of ISD. The emphasis in the literature is on systems design and the application of PETs, however, this research has shown that IS personnel see the role of managers more broadly than that and in doing so may shift the responsibility for DP from low-level technical solutions to higher-level managerial ones that ultimately have far greater potential. Management are clear regarding their role in DP provision; it is advisory, consultative and to assure data integrity and security. It is primarily one of close liaison horizontally with other IS and/or DP managers and vertically through IS structures and staff.

6.2.4 Findings in relation to the research objectives

This section considers the original research objectives in the light of the research findings. A consideration of each objective is provided in table 6.1:

<table>
<thead>
<tr>
<th>Research objective</th>
<th>Research findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective 1: Establish actual levels of PDP awareness amongst IS personnel within a small number of UK based organisations.</td>
<td>In the survey, awareness amongst respondents were reported as high, but their perceptions are that awareness amongst their colleagues was much lower. The case study research found that awareness was reported as being at a low or at an 'appreciation' level. IS personnel in these organisations were far less willing to make strong claims to DP awareness than the survey respondents did. This may be because: 1. They are genuinely less knowledgeable. 2. They are interpreting their knowledge levels in a less generous way than survey respondents did. 3. Survey respondents may be overstating their levels of awareness due to the remote nature of a survey. 4. Survey respondents may be more aware because they</td>
</tr>
</tbody>
</table>
are more involved in DP than the more general body of IS personnel that contributed to the case study research. However, the case study findings are that levels of PDP awareness are low and marginal to ISD practice.

**Objective 2: Identify and explore the attitudes and perceptions IS personnel have with regard to their role in the provision of PDP and assess the impact these have on the IS development process.**

The key findings in this area are, as already stated, a stated willingness to support PDP through ISD practice but at the same time devolving all responsibility other than systems and data security to the client or 'data owner'. A consequence of this is that PDP has yet to make a real impact on the IS development process and this is an area that the author of this thesis will continue to address.

**Objective 3: Identify the extent to which IS personnel are aware of their legal responsibilities to use privacy enhancing technologies and strategies.**

Those that contributed to the case study research were acutely aware of the need to apply security to the data in their charge but were not aware of this being a requirement of principle seven of the 1998 DPA. Comments such as 'we are data people, ..... we care for data, ..... it’s in everything we do', were not uncommon. Once presented with the list of principles most contributors were able to quickly identify the ‘security’ principle as the one that they felt most able to support.

**Objective 4: Identify which stages and practices within the systems development process IS personnel feel they have a PDP contribution to make.**

In both the survey and case study data the stages that are most frequently identified as offering the greatest opportunity for PDP leverage are the ones that occur early in a development and in the practices that span the entire lifecycle. In the survey data, systems analysis and systems design were the two most frequently identified stages with implementation and project initiation in third and fourth place respectively; in other words the entire lifecycle. The identification of these stages is supported by the case study data. It was frequently stated that DP
had to be considered as early in the development process as possible. The identification of which personnel can contribute the most to DP supports the view that DP is a whole lifecycle issue. In section 5.5.5.3 the roles identified by case study respondents as those who can contribute the most, provide lifecycle coverage in that Project Managers, Business/Systems Analysts, Systems Designers and Developers are dominant.

<table>
<thead>
<tr>
<th>Objective 5: Explore the relationship between Data Protection Officers (DPOs) and IS personnel in the provision for and management of PDP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The survey data suggests a strong relationship between IS personnel and DPO in organisations. It was shown that in many organisations responsibility for DP is either wholly or partly carried out by IS personnel. The case study findings support this view. In the case study authorities DP had until recently been the responsibility of the IS provision, whilst in LA1 it is still managed by the ITM as a shared responsibility. This confirms the important role IS personnel have in providing PDP in organisations. In the two authorities that have separated the IS and DP roles there still exists a stated close relationship between the two functions, but there is no real evidence of DP and IS coordination regarding DP and in particular within the ISD process.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objective 6: Improve the provision for PDP by enabling the wider distribution of examples of good PDP practices in organisations and the systems development process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is an objective that was not met to a satisfactory degree and this is considered further in sections 7.5. And 7.6.</td>
</tr>
</tbody>
</table>

Table 6.1: Research findings in relation to the research objectives
### 6.2.5 Findings in relation to the theoretical propositions

The theoretical propositions are the articulation of the issues that underpinned the case study research; they define the state of affairs that was either expected to be found or which the research sought to investigate the existence of. It is not surprising to see that many of these propositions are similar to the research objectives considered in the previous section.

<table>
<thead>
<tr>
<th>Theoretical proposition</th>
<th>Research findings</th>
</tr>
</thead>
</table>
| **Theoretical proposition 1**  
There is a commitment amongst IS personnel to support DP. | There is an acceptance of the responsibility to contribute to DP amongst IS personnel. This finding from earlier research (Howley, 2002) has now been confirmed both in this research and by other surveys (for example, Prior 2005, p21). |
| **Theoretical proposition 2**  
Organisations face similar challenges in responding to DP regardless of size and complexity. | Even though the three organisations that contributed to this research varied considerably in size, organisation and responsibilities, they consistently reported similar concerns and interpretation of the challenges that face them, and how to respond to those challenges. However, the overall finding with regard to challenges is that DP was no longer seen as the main challenge. These organisations are all subject to national initiatives and it was frequently noted that the concern of these staff is the most recent initiative from Government. During the period this research was conducted these included the impending Children’s Act (and in particular, the data sharing aspects of it), Freedom of Information and E-Government. |
| **Theoretical proposition 3**  
Levels of awareness may be less than required to effectively respond to DP | ‘Levels of awareness’ are frequently reported as an issue for those involved in this study. Obviously, care has to be taken drawing conclusions based on such deeply qualitative expressions, however, in the area of DP and |
challenges. specifically systems development strategies for compliance it is felt that awareness could be increased. All these organisations have effective and comprehensive provision for general DP induction and training, but in the field of IS development there is much still to be done before the era of the ‘ethical engineer’ is with us.

**Theoretical proposition 4**
Levels of commitment amongst IS personnel may vary in a consistent manner at different levels.

There is some evidence in the data that the more senior you are, the more likely you are to accept DP as a legitimate concern of IS personnel. Willingness to accept a responsibility for DP by senior IS personnel may have more to do with the history of DP in their organisation and/or political expediency than actual commitment. Both of these responses are perhaps reasonable from a pragmatic point of view.

**Theoretical proposition 5**
Little is being done to embed DP practices in systems development processes.

This proposition is fully supported by the data. Security is recognised and well provided for, but it was agreed that much more can be done across all stages and in supporting all principles. This will become a future research activity.

<table>
<thead>
<tr>
<th>Theoretical proposition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4</strong></td>
<td>There is some evidence in the data that the more senior you are, the more likely you are to accept DP as a legitimate concern of IS personnel. Willingness to accept a responsibility for DP by senior IS personnel may have more to do with the history of DP in their organisation and/or political expediency than actual commitment. Both of these responses are perhaps reasonable from a pragmatic point of view.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>This proposition is fully supported by the data. Security is recognised and well provided for, but it was agreed that much more can be done across all stages and in supporting all principles. This will become a future research activity.</td>
</tr>
</tbody>
</table>

Table 6.2: Research findings in relation to the theoretical propositions

There is considerable agreement between the findings of the survey and case study research. They both show similar results with regards to which IS personnel can contribute and when, within a traditional SDLC. The more detailed insights gained during the case study research, however, shows that little is actually being done to embed PDP into IS practice and given the lack of awareness and confidence with regard to PDP that exists, it is likely that little will be done without significant leadership and determination by both IS and DP managers. The proposals for future research outlined in section 7.6 aims to support these managers to provide that leadership.
Chapter 7: Conclusion, review and critical evaluation

7.1 Research aims, questions and original contribution

This research makes an original contribution to knowledge in the following ways:

1. Discovering and documenting the involvement by IS personnel in the provision for PDP. In doing this the research has, for the first time, recorded the views of IS personnel with regard to their perceived responsibilities for the provision of PDP.
2. Exploring and recording the attitudes of IS personnel with regard to their role in providing for DPD in organisations and systems. The attitudes discovered and explored show a willingness by IS personnel to support PDP through their professional practice, but at the same time a range of barriers were identified that may limit this support.
3. The stages in the ISD process within which IS staff feel they can contribute to PDP were discovered and documented.
4. This research has shown and explored how a lack of awareness about PDP in general and how it can impact on the ISD process in particular, may limit the provision of PDP within organisations and the ISD process.
5. The research has shown for the first time the narrowness with which some IS personnel define their PDP responsibilities and has explored the implication of this. Many respondents in this research regard security as being synonymous with DP. This restrictive view may limit the impact of PDP legislation and the contribution that can be made by a broader range of participants.
6. This research identified a lack of vision amongst these IS professionals regarding how they can contribute to PDP. The IS personnel in this research are willing to develop more PDP sensitive practices but cannot identify what needs to be done, or how, once the artificial boundary of security is removed.
7. Recording and exploring the tendency of these IS personnel to pass PDP responsibility to others within their organisations.
8. The research has documented the tensions that exist between ‘PDP professionals’ in organisations. For example, DPOs were highlighting the importance of IS
personnel within their organisation whilst at the same time their IS personnel were actively seeking to minimise any PDP responsibility.

9. The important role that IS management are perceived to have in the provision for PDP at all stages of the ISD process was identified, documented and explored.

These represent a unique contribution to the body of knowledge within the field of IS professional practice.

7.2 Evaluation of the research process

7.2.1 Methodological context

This research has been methodical and grounded in good, informed research practice. Throughout, each major methodological decision has been supported by the literature relating to that decision making context. The choices made with regard to the use of a survey and case study research are well grounded in the literature and have proved to be effective in that they have produced data that has been of sufficient quality to facilitate analysis.

Particular strengths of this research include:

1. Thorough and detailed case study design and the supporting case study protocol.
2. Effective piloting of both survey and case study research instruments.
3. The process of finding cases to participate in the research and the support given to respondents throughout the research.
4. Data analysis procedures.

Methodologically there are some aspects that benefit from further consideration, including:

1. In the case study authorities it was frequently reported that staff have to respond to the most recent government priority and this inevitably leads to less time being available to address the deeper or broader implications of other legislation that was
a priority until recently. It was reported in conversations that these changes in priorities occur with disturbing frequency and that they demand immediate attention. This influence did not emerge during the piloting of case study processes and instruments and as such the impact of this was not developed during this research.

2. In LA2 it was agreed that the respondents would include the ITM, DPO and four developers. On the day that meetings were scheduled with these developers it quickly became apparent that they were not developers, but the Managers of development teams; their concerns and perspectives were far more managerial than developmental and this significantly affected the nature of this research. The case study data design specifically sought insights from development staff to complement the managerial view obtained during the survey. It was agreed that the interviews/discussions would continue with these respondents presenting views that they felt are representative of their development teams and based on their own development experiences.

3. The case study sought insights into the views of Systems Analysts, Systems Designers and Developers rather than Managers. This was not realised to the extent hoped for and as such the views presented in this research may still be usefully be informed by further research into a non-managerial perspective.

4. The other methodological issue that needs considering here concerns the close monitoring of the research by the ITM in LA2. The meetings with the four DTLs were all conducted on the same day and consisted of a guided discussion/interview lasting approximately one hour and a more general conversation over lunch. The ITM announced in the morning that he wanted to be present in the meeting room the whole time, in case he ‘could add useful context or background information’. It was suggested by the researcher that this was perhaps too generous an offer, to give another whole day of his time to this research, but he insisted on remaining in the room, and indeed, everywhere else the researcher went throughout the entire day. At the end of the time spent with this authority it was inevitable that the researcher considered how the responses may have differed if the line manager of respondents had not been present the whole time.

5. Awareness of DP was an issue that was addressed early in the interview process and most respondents reported that their knowledge is not high. It was later considered whether or not the early introduction of the topic may have promoted a defensive
attitude and contributed to many staff retreating to the relative safety of, ‘it’s their responsibility’ and the focus on security.

7.2.2 Data analysis aspects

The process of data analysis for both the survey and case study data is regarded as effective. The data analysis strategy was documented and refined prior to piloting and then reviewed following the scoping studies. This process led to changes in both the research instruments and the researcher’s style and procedures. These changes resulted in the researcher having much greater confidence in the research process and its instruments and this in turn enabled the researcher to approach the research task with greater confidence and with the ability to exercise less control over the research process whilst at the same time ensuring that discussions remained pertinent to the research aims, objectives and propositions.

7.3 Evaluation of the research findings

The findings of this research are significant in a number of important aspects. Firstly they provide insights for the first time into how IS professionals have responded to a piece of legislation for which they are identified as being critical to its aims being realised. These insights have shown that the aspiration of the IC for the application of PETs by ‘ethical engineers’ is not yet universally realised. Indeed, there is considerable ambiguity regarding responsibility for DP within the case study organisations and this is an issue which will limit the development of privacy sensitive systems.

The research identified which stages and which IS personnel are seen as offering the greatest opportunity for PDP leverage, however, there is little beyond that regarding what these staff can actually do within these stages. Other than a general reliance on ‘apply security’, the IS personnel in this study had not identified or applied specific
development practices and procedures that explicitly address PDP with the ISD process\textsuperscript{15}. This issue is addressed further in section 7.5 below.

The research has also identified the importance of attitudes, awareness and commitment. No legislation will be implemented as effectively as it might without these issues being addressed. DP systems are systems that necessarily involve people and people must therefore be at the forefront of our provision for DP; we cannot rely on technology alone.

\textbf{7.4 Research achievements}

The main achievements of this research are identified in section 7.1 above but it is also notable in that:

1. Two of the organisations that took part in the case study research are planning to develop procedures and strategies for the greater involvement of DP and the DPO in their development processes.

2. One of those organisations has invited the researcher back with a view to exploring how the research instrument used in the second scoping study can be used to identify DP opportunities within their ISD practices.

3. This research has positively influenced undergraduate teaching in the School of Computing at De Montfort University. A final year undergraduate module called Privacy and Data Protection was introduced by the lead researcher in 2001 with a view for it to provide a vehicle through which the issue of PDP can be explored within an undergraduate computing and IS curriculum. The module has become the most popular fifteen credit option final year module\textsuperscript{16} within the School and it has maintained that position for many years. This research is instrumental in directing both technical and business computing students to view their IS/IT roles and responsibilities within a framework that is sensitive to and reflective of PDP practices.

\textsuperscript{15} For example minimalist data visibility, minimising data capture, including attributes in databases that support DP related processes such as use-by and remove-by dates, data relating to Subject Access Requests, the date the data was last checked for accuracy, etc.

\textsuperscript{16} The module attracts in excess of eighty students each year.
4. The research has raised the profile of DP as a key development issue through the publication of three conference papers and an article in the IMIS Journal (see Appendices 13, 14, 15 and 16).

7.5 Significance and limitations of the findings

The process of undertaking this research and the dissemination of its findings are informing the IS community of the ongoing importance of DP in systems design and at the same time providing opportunities for this issue to be considered.

This research has shown how awareness of DP in general and its ISD implications are little known or understood, beyond the blanket response of ‘apply security’. The implications of this are that a large number of opportunities are being lost or missed and that much more can and perhaps should be done to bring about greater PDP within systems and during their development. Because of this lack of awareness the research did not find evidence of the application of privacy enabling strategies to identify and disseminate as examples of good practice. Beyond the application of security there is a paucity of ideas within the organisations studied.

As already stated, the survey findings are based on the views of managers in large organisations. The views of others were considered and are reported here but the research findings are limited by the higher number of managerial respondents in the case study organisations than was planned for. The findings are limited in terms of the small number of cases participated in this research and the limited scope of their business activities.
7.6 Further research in this field

Many areas for future research have been identified and these are presented below:

1. Research into the interface and relative responsibilities between IS personnel and the end-user in the ISD process. This would allow for an exploration of the relative responsibilities of personnel with regard to PDP and further inform a finding of this research that IS personnel see DP as the responsibility of the user.

2. Undertake action research in the area of DPO interventions into the ISD process with a view to exploring and refining the contribution that DPO can make as part of ISD.

3. Undertake a further survey of Systems Analysts, Systems Designers and Developers to seek their 'operational' view of the provision for PDP both within organisations and during the ISD process.

4. Further develop the second scoping study instrument (see section 3.8.3) applying it within organisations as in-house training with a view to seek out and/or developing exemplars of good PDP practice. Staff in LA2 have agreed that this is an exercise they would be willing to support.

7.7 Concluding remarks

The findings reported in this thesis represent the start of an ongoing research plan. This research has established that IS personnel, their managers and DPOs are all willing to engage in the process of providing PDP through IS practice and that when guided they can suggest ways of realizing this. The author of this thesis is committed to undertaking a range of research consultancy activities during the coming years that identify, pilot and publish the details of a range of privacy enhancing development strategies that can be employed by IS personnel in a range of settings.
References


BCS (1996b) BCS Data Protection Committee Terms of Reference [WWW] Available at: http://www.bcs.org.uk/dataprot/tor.htm [Accessed 18/5/00]


[Accessed 12/7/07]


Dowding, K. (2001) *There must be an end to the confusion: Policy Networks, intellectual fatigue and the need for political science methods courses in British universities* Political Studies Vol. 49 No.1 March 2001 p89-105


EPIC - Electronic Privacy Information Centre (1999) *Overview* [WWW] Available at:


HMSO (1972) Younger Committee - Report of the Committee on Privacy, Cmnd. 5012


IC (2006) Report on IC Annual Track [WWW] Available at:
Organisation data:
Individual data:

ICDPPC (2005) The Montreux Declaration [WWW] Available at:
http://www.edsb.ch/e/links/international/konferenzen/2005/montreux_declaration_e.pdf  [Accessed 1/10/05]

ICO April 2006 Data Protection Technical Guidance Note: Privacy Enhancing Technologies (PETs) [WWW] Available at:


http://website.lineone.net/~peter.john/polnet2.html  [Accessed 15/3/02]


Krippendorff, K. (1980) Content Analysis An Introduction to its Methodology SAGE


Mason, J. (2002) Qualitative Researching 2nd Ed SAGE


Popper, K (1979) Objective Knowledge An Evolutionary Approach Revised Edition

Preece, R. A. (1994) **Starting Research: An Introduction to Academic Research and Dissertation Writing** Pinter Publishers


Privacy and Data Protection (2000) ‘**Website Processing Unlawful**’ (October 2000)
Published by Privacy and Data Protection Ltd


Shorts, E., de Than, C (1998) **Civil Liberties Legal Principles of Individual Freedom** Sweet and Maxwell

Silverman, D (2000) **Doing Qualitative Research** SAGE

Stake, R. (1995) **The Art of Case Research** SAGE


**The Computer User Year Book** (2003) Published by VNU Business Media Europe


Appendix 1: De Montfort University - Ethics form for survey research

De Montfort University
Faculty of Computing Sciences and Engineering
Advance approval of activities involving human research ethics

Title of Activity: PhD Research titled ‘An investigation into the role of Information Systems personnel in the provision for privacy and data protection’

Researcher / Student Name: Richard Howley

Supervisor Name: Prof. S Rogerson, Dr. N.B Fairweather, and Dr. L Pratchett

Brief description of activity objectives:

Research Aims, Questions and Objectives

The aim of this research is to investigate the role of IS personnel in the provision for data protection at both information systems and organisational levels. This research will identify both actual and perceived roles that IS staff have with regard to PDP and address the following research questions:

1. What is the role of IS staff in the provision for PDP within systems and organisations?
2. How aware are IS staff of the PDP obligations on them and their organisations?
3. What explanations exist for current levels of awareness?
4. What aspects of IS professional practice have PDP enhancing opportunities and how widely known or applied are these?

In addressing these research questions this research will have as objectives:

1. Establish actual levels of PDP awareness amongst IS staff within UK based organisations.
2. Identify and explore the attitudes and perceptions IS staff have with regard to their role in the provision of PDP and assess the impact these have on the implementation process.
3. Identify the extent to which IS staff are aware of their legal responsibilities to use privacy enhancing technologies with systems.
4. Collate examples of good practice with regard to the use of privacy enhancing technologies and practices in systems development and produce a set of guidelines for use by the IS profession.

Methods used in the proposed research include questionnaires, interviews, case study and focus group sessions.

A potential ethical issue that may need particular attention concerns the requirement for professional IS staff to undertake an honest appraisal of their awareness of PDP issues. Some respondents may feel that this information could be potentially damaging to their professional standing; admitting to low levels of awareness of an issue that we are increasingly seen as being responsible for may be professionally uncomfortable. The ethical issues here mean that respondents must be assured of confidentiality of their responses and adequate measures will be applied to assure security of identifiable (even if only marginal) data. In order to secure the reliability, and therefore ‘ethicalness’ of the research results measures must be built in to seek from respondents a non-defensive approach to self-appraisal.

Respondents and case study organisations will be informed of the need for absolute confidentiality and that this will be maintained throughout the research and in any published results. This information will be provided at the point at which respondents and organisations agree to participate in the research, thereby further assuring informed consent.

A detailed consideration of ethical aspects of the proposed research is included in chapter six of the transfer document and in particular twelve action points are provided that assure on-going ethicalness.
If the review of the activity results in major ethical issues being identified (outcomes 3 or 4) describe the issue(s) and procedures in place to address them (outcome 3 only)

No major ethical issues identified.

Advance approval of activities involving human research ethics

Review of activity

Has the research proposal identified any of the following research procedures?

1. Gathering information about human beings through: Interviewing, Surveying, Questionnaires, Observation of human behaviour
2. Using archived data in which individuals are identifiable
3. Researching into illegal activities, activities at the margins of the law or activities that have a risk of injury

If any of the above occur does the proposal satisfactorily identify the ways in which the researcher / student will be dealing with the following (tick boxes for “YES”):

- Providing participants with full details of the objectives of the research
- Voluntary participation with informed consent
- Written description of involvement
- Freedom to withdraw
- Keeping appropriate records
- Signed acknowledgement and understanding by participants
- Consideration of relevant codes of conduct

Do the procedures identified necessitate formal assessment? YES / NO
If so has the assessment been carried out? YES / NO

Other factors that could/will give rise to ethical concerns

There are four possible outcomes from reviewing the activity against the three categories and the procedures in place:

- no ethical issues
  1. minor ethical issues which have been addressed and concerns resolved
  2. major ethical issues which have been addressed and concerns resolved
  3. ethical issues that have not been resolved

Tick the outcome of the review: 1 ☐  2 ☐  3 ☐  4 ☐
Authorisation

- The reviewer authorises those activities in the first three outcomes.
- Activities in the third outcome are reported for information only to the Faculty Committee.
- Activities in the fourth outcome are submitted to the Faculty Committee for resolution.

signature of researcher / student  
signature of supervisor  
authorising signature  

(date)  
(date)  
(date)
Appendix 2: De Montfort University - Ethics form case study research

De Montfort University
Faculty of Computing Sciences and Engineering
Advance approval of activities involving human research ethics

Title of Activity: Case study research into the role of IS staff in the provision for Privacy and Data protection in systems and organisations.

Researcher / Student Name: Richard Howley

Supervisor Name(s): S. Rogerson, NB Fairweather & L Pratchett

Brief description of activity objectives:
Three case study investigations are to be undertaken into the contribution that IS staff can and do make to the provision of privacy and data protection (PDP) in organisations and within information systems. The studies will also seek insights into the management contribution to this process.

The research methods used will be:
Interviewing IS staff and Data Protection officials.
Reviewing systems analysis and design models/documents.
May involve observing system practice (as required and offered by case study respondents).

All respondents will be provided with written details regarding:
a. The aims and nature of the research.
b. FAQ’s leaflet (see attached) that explains in more detail what is required of participants.
c. The voluntary nature of the research.
d. The opportunity and procedure to withdraw at any time from the research and confirmation that all data provided by them will be destroyed.
e. How the data they provide will be used.
f. Confidentiality of the data any individual or organisation provides. All data, materials and records provided will be kept secure in locked storage and destroyed once the research is completed or by the end of 2005 at the latest.
g. Details of the risks and benefits of participating in the research (on the Consent Form – see attached).

All respondents will be required to sign a Consent Form (attached) approving their involvement in the research and confirming that they are taking part voluntarily and that they are aware of the opportunity and procedures to withdraw from the research. The research will be conducted in accordance with current ‘Codes of Practice’ that exist to guide research of this type. Drawing on the contents of many codes the following aspects will be significant in the design, implementation and analysis of this research:

<table>
<thead>
<tr>
<th>Respect for participants privacy</th>
<th>Open and fair data gathering techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective management of the research analysis</td>
<td>Openness and transparency in research design and analysis</td>
</tr>
<tr>
<td>Voluntary participation</td>
<td>Communicate the aims of the research to participants</td>
</tr>
<tr>
<td>Secure storage of data</td>
<td></td>
</tr>
</tbody>
</table>

If the review of the activity results in major ethical issues being identified (outcomes 3 or 4) describe the issue(s) and procedures in place to address them (outcome 3 only).

17 UK Qualifications and Curriculum Council Research Code of Practice, Strathclyde University Code of Practice, DEFRA - Code of Practice for the Quality Assurance of Research, etc.
Advance approval of activities involving human research ethics

Review of activity

Has the research proposal identified any of the following research procedures?
1. Gathering information about human beings through: Interviewing, Surveying, Questionnaires, Observation of human behaviour
2. Using archived data in which individuals are identifiable
3. Researching into illegal activities, activities at the margins of the law or activities that have a risk of injury

If any of the above occur does the proposal satisfactorily identify the ways in which the researcher / student will be dealing with the following (tick boxes for “YES”):
- Providing participants with full details of the objectives of the research
- Voluntary participation with informed consent
- Written description of involvement
- Freedom to withdraw
- Keeping appropriate records
- Signed acknowledgement and understanding by participants
- Consideration of relevant codes of conduct

Do the procedures identified necessitate formal assessment? YES/NO
If so has the assessment been carried out? YES/NO

Other factors that could/will give rise to ethical concerns

There are four possible outcomes from reviewing the activity against the three categories and the procedures in place:
1. no ethical issues
2. minor ethical issues which have been addressed and concerns resolved
3. major ethical issues which have been addressed and concerns resolved
4. ethical issues that have not been resolved

Tick the outcome of the review: 1 2 3 4

Authorisation
- The reviewer authorises those activities in the first three outcomes.
- Activities in the third outcome are reported for information only to the Faculty Committee
- Activities in the fourth outcome are submitted to the Faculty Committee for resolution

signature of researcher / student  date
signature of supervisor  date
authorising signature  date
Appendix 3: Case study consent form for participants to read and sign

Consent Form
Centre for Computing & Social Responsibility

An investigation into the role of Information Systems staff in the provision for privacy and data protection

Staff from the Centre for Computing and Social Responsibility (CCSR) are undertaking research into the contribution that Information Systems (IS) staff can and do make to the provision of privacy and data protection (PDP). You have been selected as a potential participant due to your organisation meeting the selection criteria for inclusion. Please read this form and the attached ‘Frequently Asked Questions’ leaflet before agreeing to take part in this study. Feel free to ask any questions that you may have that are not answered in this form or on the FAQ’s leaflet. To ask any questions or to seek further clarification of any issue related to this research please contact the Lead Researcher using the contact details provided below.

Who should read this document?
All those considering participation in this important research. This is likely to include at least two categories of individuals:
1. Organisational staff that have the authority to represent the organisation or departments within it. Individuals in this category are likely to be considering whether the organisation or department wishes to participate in the study.
2. Individual respondents that may have been asked to participate by their managers or colleagues.

Lead Researcher
Richard Howley (Principal Lecturer in Information Systems and Research Associate in the Centre for Computing and Social responsibility at De Montfort University, Leicester)

Contact Details
School of Computing, De Montfort University. The Gateway. Leicester LE1 9BH
Tel: 0116 207 8268 Fax: 0116 207 8159 Email: rgh@dmu.ac.uk

Research team
Richard Howley, Professor Simon Rogerson, Dr NB Fairweather and Dr L Pratchett

Background information
During the last 10 years there has been a considerable amount of legislation passed in the area of privacy and data protection. In the literature that has accompanied these developments IS staff are frequently seen as key providers of the technical expertise needed for PDP. This research seeks to explore the views of IS and data protection staff regarding how PDP can be, and is, facilitated through their professional practice.

Valid contributions to this research can be made both by organisations that have highly formal PDP processes and by those organisations that are still considering how to respond to the challenges of PDP.
Activities you will be asked to take part in

If you agree to contribute to this research you will be asked to:

1. Answer a series of interview questions regarding how PDP requirements are expressed in your professional practice. This interview is designed to last between 45 minutes and one hour.
2. Read and approve the transcript of the interview.
3. You may wish to support your answers to questions by reference to documentation that evidences practices that support PDP. In this situation you may be asked to provide examples of such documents and, of course, you can decline any such request.
4. It is hoped that within each organisation taking part in the study interviews will be undertaken with the person responsible for Data Protection, the Head of Computing and between 1 and 3 systems development staff.

Research dates

It is anticipated that interviews will be undertaken during September and October 2004. The final project report will be completed and sent to participants by end of December 2004.

Risks of participating in the study

The risks involved in participating in this research may include:

1. You may feel that your professional knowledge or expertise is being assessed. It is not. This research is about finding out how something is either done or could be done. Even if you do not explicitly consider PDP in your professional practice at this moment in time we want to find out your views of how it should or could be done.
2. The results of this study may be published in reports, academic journals and trade publications and subject to your approval your organisation will be named in order to express the appreciation of the researchers and in order to increase the validity of the research. You will be given the opportunity to review and contribute to any material about to be published that explicitly contains comments about your particular organisation or individuals within it.
3. You may be asked questions which you do not feel that you can satisfactorily answer. It is anticipated that each respondent will not have answers to some of the questions asked and as such not having answers for all questions is no reflection of skills or ability.
4. In some organisations supervisors or managers may identify staff by the nature of the comments made. Conversely, staff may identify supervisors or managers in organisations by the description of the organisation and the relatively few managers taking part in each organisation. These opportunities to identify personnel from their comments cannot be removed from the research and the publication of its findings. It is hoped however that those contributing to the research will be working in organisations characterised by openness and a willingness to share ideas in a non-defensive manner and in these types of organisations we hope that this ‘risk’ to taking part will be less important that it may be in other organisations. You will, of course, be invited to express any confidentiality concerns you may have in accordance with the provisions outlined in the section on ‘Confidentiality’ below.

Benefits of participating in the study

Benefits include:

1. Involvement provides you with the opportunity to reflect on your own professional practice in response to these important developments.
2. Your organisation will be amongst the first to receive a copy of the research report. This report will include a set of guidelines gathered from respondents and other research into how to more effectively develop systems for data protection compliance.
3. You will be contributing significant insights into an important and growing area of IS professional practice. These insights will be used to inform systems development practice across the IS profession.
4. Your organisation can request from the research team one of the following:
   a. A management briefing regarding your organisation’s response to current legislation.
   b. A staff development seminar regarding current good practice in the development of privacy/data sensitive systems.
   c. A written report outlining and evaluating your systems development practice in the context of developing systems that are compliant with an ever increasing range of data legislation.
Confidentiality

Confidentiality and sensitivity to the rights of the organisation will be of paramount importance to the research team. We are committed to making every effort to meet and support your personal confidentiality needs.

It is anticipated that the organisation will agree to be identified as contributing to the research but no specific comments or conclusions will be attributable to any one named organisation. As already stated, organisations will be referred to through the use of a pseudonym (ie. ‘organisation 1’, ‘2’, etc.).

All interview responses will be kept strictly confidential. No comments made will be attributable to any named individual. The names of individual respondents will not be made public; rather a coding system will be used such as ‘Organisation 1, respondent A’. However, certain professional details will be requested from all respondents and this may enable individuals to be identified by those that work closely with them. Details such as job title, length of time in the job, etc, will be requested in order to provide the necessary contextual information for effective data analysis.

Recordings of interviews, transcripts and any documents passed to members of the research team will be kept in a secure manner and not released or published in any manner without the written permission of the organisation or individual that provided it. The research team are aware of the ‘legal limits to confidentiality’ but do not anticipate that this will be relevant to this research.

Voluntary nature of the research

Your contribution to this study is entirely voluntary. Your decision to take part or not will not affect your current or future relationship with the CCSR or De Montfort University. It is a condition for participating organisations that the participation of individuals within the organisation is similarly voluntary. If you do decide to contribute, you are free to withdraw at any time. This can either be at an organisational or individual level. If the organisation decides to withdraw from the study you have the right to request that any data collected from all members of your organisation is destroyed and not processed further. If the request to withdraw is from an individual within an organisation then they have the right to request that the data they personally provided is destroyed and not processed further. In either event, all material held by the researchers relating to withdrawing organisations or individuals will be destroyed.

Procedure for withdrawing

Should you decide to withdraw from the study you may do so by providing a written request to the Lead Researcher. You do not have to provide any reason or justification for your decision. This notification should be sent by post or by email and confirmation of receipt will be sent to you as soon as is practicable. Following receipt of notification to withdraw all data relating to the organisation or individual will be destroyed. Notification of its destruction will be sent to the organisation or individual as soon as is practicable following its actual destruction.

Any other concerns

Should you have any questions or concerns that the research team can assist in answering or addressing please do not hesitate to contact the Lead Researcher, Richard Howley at rgh@dmu.ac.uk or by telephone on 0116 207 8268. We will make every effort to respond to your concerns or questions quickly, honestly and clearly. We really do want your contribution, but only in a fully informed and voluntary manner.
Whether you decide to participate in this important study or not, members of the research team appreciate your consideration of this matter. Having read this document to this point is worthy of our expression of appreciation! This is necessarily a long document because of our commitment to providing sufficient information for you to:
1. appreciate our professional commitment to this research and to safeguarding your data, and
2. to enable you to make an informed choice whether to participate or not.

Statement of Consent
I have read this Consent Form and the FAQ’s leaflet and I have been given the opportunity to ask any further questions about this research. I consent to participating in this research and to the recording of the interviews as described in this document.

Please sign as an individual participant or as the organisation’s representative, or as both.

Signed (Organisational Representative): ___________________ Date: _______
Signed (Study Participant): ________________________________ Date: _______
Signed (Researcher): ________________________________ Date: _______

A copy of this signed document will be sent to all participants for their records.
A Case Study Protocol

for the

Design and Management

of

Case Study Research

What is a case study protocol?

A protocol is a means of recording the essential details that are needed to effectively support case study research. It is a document that sets out a set of prompts and or questions that must be considered as part of an effective research design. However, it is more than a design document. It serves as a supportive framework within which the actual research is undertaken and the results recorded. It also requires the researcher to evaluate the protocol once the research is completed; in this respect the protocol supports the entire research process. It enforces rigour and discipline in the design of research and provides a structured mechanism for the researcher to address the important aspects of design that may otherwise be omitted.

This protocol supports the case study research that sought insights into:

The role of Information Systems professionals in the provision for privacy and data protection within organisations, systems and the systems development process

Richard Howley @2004
De Montfort University
rgh@dmu.ac.uk
## Background and context for the research

<table>
<thead>
<tr>
<th>Issue</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the research project</td>
<td>PhD into the role of IS personnel in the provision for PDP within organisations, systems and the systems development process.</td>
</tr>
<tr>
<td>Lead researcher name and contact details.</td>
<td>Richard Howley Research Associate of the CCSR School of Computing De Montfort University Leicester LE1 9BH Tel: 0116 207 8268 email: <a href="mailto:rgh@dmu.ac.uk">rgh@dmu.ac.uk</a></td>
</tr>
<tr>
<td>Other researchers, supervisors or support staff.</td>
<td>Prof. Simon Rogerson (Director of CCSR) Dr. N.B. Fairweather (Research Fellow in CCSR)</td>
</tr>
<tr>
<td>Project start and end dates.</td>
<td>Field work - September – November 2004 Data analysis – January – June 2005</td>
</tr>
<tr>
<td>Provide details of funding authority.</td>
<td>None</td>
</tr>
<tr>
<td>What is the background to the research?</td>
<td>This research builds on the survey undertaken in 2002 into the role of IS personnel in the provision for PDP. That research was reported at ETHICOMP 2002 in Lisbon (for further details see the published paper available from the CCSR). The survey provided insights into which IS personnel can contribute to PDP and when in the IS development life cycle; this case study research seeks to explore these themes in more detail.</td>
</tr>
<tr>
<td>What are the case study research aims? These may be expressed as case study propositions, research questions and/or hypothesis.</td>
<td>This case study research addresses three research questions: 1. What is the role of IS personnel in the provision for PDP within systems and organisations and how aware and accepting are they of their obligations? 2. What aspects of IS professional practice have PDP enhancing opportunities and how widely known or applied are these? 3. What is the role of IS management in the provision for PDP and how does that interface with other DP managers in organisations?</td>
</tr>
<tr>
<td>What is the literary context of the case study?</td>
<td>Most literature in this area focuses on PETs and Systems design as the main areas in which IS personnel can contribute to PDP. This research seeks confirm or otherwise this belief and to add detail to this high-level presumption.</td>
</tr>
<tr>
<td>What is the theoretical context for the research?</td>
<td>This case study research is guided by the following theoretical propositions: 1. There is a commitment amongst IS personnel to protect data and to provide data privacy. 2. Organisations face similar challenges in responding to DP regardless of their size and complexity. 3. Levels of awareness may be less than that required to effectively respond to the DP challenges. 4. Rapid changes in the legislative context may inhibit commitment to DP. 5. Levels of commitment may vary in a consistent manner at different occupational levels. 6. More can be done to embed PDP practices in the systems development process.</td>
</tr>
<tr>
<td>Has an ethical review been undertaken and the outcome approved?</td>
<td>Yes. Undertaken and Approved by Prof. S Rogerson and Dr. N.B. Fairweather Summer 2004.</td>
</tr>
</tbody>
</table>
## Case Study Set-up

<table>
<thead>
<tr>
<th>Is the case study:</th>
<th>detailed descriptions and analysis of professional practice in the provision of PDP, providing new insights into current IS practice in the provision for PDP. In this respect the research exhibits features of the explanatory case study type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. exploratory</td>
<td>this research is a descriptive case study that will result in the production of ‘thick descriptions’ of phenomena.</td>
</tr>
<tr>
<td>ii. descriptive</td>
<td></td>
</tr>
<tr>
<td>iii. explanatory</td>
<td></td>
</tr>
<tr>
<td>iv. other</td>
<td></td>
</tr>
</tbody>
</table>

| Will the study be a single or multiple case studies? | Multiple – 3 cases. Reasons include: 1. The multiple case justification: ‘the study of innovation in organisations' applies here. 2. Multiple cases supports ‘literal replication’ that will provide ‘more compelling evidence’. 3. Using multiple cases increases external validity. 4. Multiple cases are within the limited resource capabilities of this research. 5. Given the limited resources available for this research any increase in the number of cases would result in a reduction in the depth of analysis that could be undertaken within each case. |

<table>
<thead>
<tr>
<th>Is there one or more unit of analysis?</th>
<th>Two units of analysis in each case.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>What is/are the unit(s) of analysis?</th>
<th>1. The role of IS development staff in providing PDP in the systems development process. 2. The management of PDP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>What industry sector is the case study from and why?</th>
<th>UK local Authorities …. because: Large data controllersprocessors. DP policies are likely to exist. Accountable for data policies and should therefore be active in considering DP. Access less problematic than some other sectors.</th>
</tr>
</thead>
</table>

## Data Collection Plan

<table>
<thead>
<tr>
<th>Issue</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What data collection strategies employed and why?</td>
<td>Individual interviews are the prime source of data capture. Interviews are to be recorded and transcribed using an independent professional secretarial services experienced in the transcription of research data. Recording the interviews allows for a permanent record of the dialogue to be kept for accuracy, checking the transcription process and allowing for the exploration of nuances, etc. Transcription, though costly and time consuming will allow for manual and software data analysis processes to be applied.</td>
</tr>
<tr>
<td>From whom will data be collected? Relate to units of analysis.</td>
<td>Data will be collected from IT Managers, IS Developers and DP Officials in all organisations. These three views, within three organisations, allows for the finding to be examined as follows:  - Personnel in the same role can be analysed together to see if there are trans organisational issues emerging. This can be referred to as horizontal-role analysis.  - Each organisation can be analysed in isolation of each other looking for intra-organisational issues. This can be referred to as vertical-organisational analysis.</td>
</tr>
<tr>
<td>How will data be stored?</td>
<td>The tapes and transcripts will be locked in a filing cabinet in the locked office of the Lead Researcher.</td>
</tr>
<tr>
<td>When and how will the data be destroyed?</td>
<td>It is anticipated that all data will be destroyed by the end of 2005.</td>
</tr>
</tbody>
</table>
### Data analysis strategy

<table>
<thead>
<tr>
<th>What data analysis strategies are used in this research?</th>
<th>Grounded theory provides the major theoretical framework within which the data analysis will be undertaken. In particular the following steps will be undertaken:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Familiarisation</strong>: Reading and re-reading data - note your reaction to the data.</td>
<td><strong>Reflection</strong>: Consider reactions in the context of previous research.</td>
</tr>
<tr>
<td><strong>Conceptualisation</strong>: Identify emerging themes even if conceptual reliability is uncertain.</td>
<td><strong>Catalogue concepts</strong>: Label and correlate emerging themes and concepts.</td>
</tr>
<tr>
<td><strong>Recording</strong>: Check the context and concepts that are used seeking consistency of results/analysis.</td>
<td><strong>Linking</strong>: Join emerging patterns to form a holistic theory for review.</td>
</tr>
<tr>
<td><strong>Re-evaluate</strong>: Involves the evaluation of theory based on a review by others.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What codes looked for in the data? Relate to units of analysis.</th>
<th>The initial set of codes are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>R Role</td>
<td>BG Background</td>
</tr>
<tr>
<td>TR Training</td>
<td>LEG Legitimacy</td>
</tr>
<tr>
<td>AW Awareness</td>
<td>EF Effectiveness of DP in ISD and Organisation</td>
</tr>
<tr>
<td>IMP Improvement strategies</td>
<td>MAN How DP is managed</td>
</tr>
<tr>
<td>LC Lifecycle stages and PDP</td>
<td>ISS IS personnel and their contribution</td>
</tr>
<tr>
<td>SD Systems development</td>
<td>SDC Systems development changes</td>
</tr>
<tr>
<td>SD/DP Systems Development with a DP emphasis</td>
<td>PR Principles</td>
</tr>
</tbody>
</table>

| Dates of data analysis. | Ongoing between September 2004 and March 2005 (and ever since!) |

<table>
<thead>
<tr>
<th>Emerging codes and themes.</th>
<th>Add new codes as data analysis continues:</th>
</tr>
</thead>
<tbody>
<tr>
<td>OD Ownership of data</td>
<td>DS Data sharing</td>
</tr>
<tr>
<td>S Security</td>
<td>EUC End-user computing</td>
</tr>
<tr>
<td>LI Liaison between data people</td>
<td>SR Shared responsibility</td>
</tr>
<tr>
<td>RM Risk management</td>
<td>CP Current priorities</td>
</tr>
<tr>
<td>ICM Inconsistent messages from government</td>
<td>DA Data audits</td>
</tr>
<tr>
<td>CUL Culture</td>
<td>EG E-Government</td>
</tr>
</tbody>
</table>

---

188
Piloting the research and instruments

<table>
<thead>
<tr>
<th>Pilot study dates</th>
<th>17 June 2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pilot study contact:</td>
<td>Paul Simpkins</td>
</tr>
<tr>
<td>Name</td>
<td>→</td>
</tr>
<tr>
<td>Role/Position</td>
<td>Senior Policy Officer (Governance)</td>
</tr>
<tr>
<td>Telephone</td>
<td>01274-433500</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:paul.simpkins@bradford.gov.uk">paul.simpkins@bradford.gov.uk</a></td>
</tr>
<tr>
<td>Pilot study organisation:</td>
<td>City of Bradford MDC</td>
</tr>
<tr>
<td>Name</td>
<td>4th Floor</td>
</tr>
<tr>
<td>Address</td>
<td>Jacobs Well</td>
</tr>
<tr>
<td>Telephone number</td>
<td>Nelson St</td>
</tr>
<tr>
<td>Fax number</td>
<td>Bradford</td>
</tr>
<tr>
<td>PS very experienced in both DP and ISD.</td>
<td></td>
</tr>
<tr>
<td>Pilot study implementation notes – that may affect analysis</td>
<td>4th Floor</td>
</tr>
<tr>
<td>Telephone number</td>
<td>BD1 5RW</td>
</tr>
<tr>
<td>Tel:</td>
<td>1274-433500</td>
</tr>
<tr>
<td>Who will be interviewed?</td>
<td>11am Senior Policy Officer (Governance)</td>
</tr>
<tr>
<td></td>
<td>11.45am Head of ICT</td>
</tr>
<tr>
<td></td>
<td>12.30am Head of Information Services</td>
</tr>
<tr>
<td></td>
<td>1.30pm A member of your development staff</td>
</tr>
<tr>
<td></td>
<td>2.15pm A second member of your development staff</td>
</tr>
<tr>
<td>Pilot study outcome – issues emerging</td>
<td>Allow for a greater degree of flexibility in session, ie. let the respondent tell their story rather than trying to force the session along the list of questions. Two respondents agreed that they do not mind pausing the dialogue to check that all the main interview issues are covered.</td>
</tr>
<tr>
<td></td>
<td>Document review of the case study letters and interview questions resulted in positive assurance that they were suitable and likely to be received well.</td>
</tr>
<tr>
<td>Changes to design resulting from pilot</td>
<td>Included prompts for SDLC and DP Principles to assure greater consistency in respondents understanding of concepts.</td>
</tr>
</tbody>
</table>
### Site 1 (if multiple case complete addition site specifications on next page):

<table>
<thead>
<tr>
<th>Name of site</th>
<th>A District Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and contact details of main contact.</td>
<td>[Removed to provide anonymity for participating organisation]</td>
</tr>
</tbody>
</table>

**Is there a need for key respondents?**

If 'Yes':

1. Has a briefing session been prepared?
2. Has it been implemented?
3. Note emerging issues.

A key respondent is not essential. The Manager agreed to make all necessary arrangements for the day, including scheduling meetings and making staff available.

**What arrangements exist for personnel in case organisation to be briefed about the research and their role?**

Head of IT will liaise with his Senior Developer. Researcher will check that briefing has taken place at the start of each session – briefing respondents as necessary.

**Who will be interviewed and when?**

Head of IT
A Senior Developer

**What arrangements exist for case study personnel to read and sign the consent form?**

Sent in advance and agreed to sign on the day.

**How will transcripts be checked by respondents?**

Final interview prompt covers this. Hopefully all will agree to read transcripts to check for accuracy and completeness.

---

**Documentation Control record for Case Study organisation**

<table>
<thead>
<tr>
<th>Interview with</th>
<th>Interview date</th>
<th>Date given for transcription</th>
<th>Back from transcription</th>
<th>Date sent for checking</th>
<th>Deadline date for changes and note of action needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of IT</td>
<td>26/10/04</td>
<td>4/11/04</td>
<td></td>
<td></td>
<td>18/11/04</td>
</tr>
<tr>
<td>Senior Developer</td>
<td>1/9/04</td>
<td>Done by lead researcher</td>
<td>14/10/04</td>
<td>4/11/04</td>
<td>18/11/04</td>
</tr>
</tbody>
</table>
Site [2]:

<table>
<thead>
<tr>
<th>Name of site</th>
<th>A County Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and contact</td>
<td>[Removed to provide anonymity for participating organisation]</td>
</tr>
<tr>
<td>details of main</td>
<td></td>
</tr>
<tr>
<td>contact.</td>
<td></td>
</tr>
<tr>
<td>Is there a need for</td>
<td>Not needed. Group briefing sessions arranged at the start of the interview day.</td>
</tr>
<tr>
<td>key respondents?</td>
<td></td>
</tr>
<tr>
<td>If 'Yes':</td>
<td></td>
</tr>
<tr>
<td>1: Has a briefing</td>
<td></td>
</tr>
<tr>
<td>session been</td>
<td></td>
</tr>
<tr>
<td>prepared?</td>
<td></td>
</tr>
<tr>
<td>2: Has it been</td>
<td></td>
</tr>
<tr>
<td>implements?</td>
<td></td>
</tr>
<tr>
<td>3: Note emerging</td>
<td></td>
</tr>
<tr>
<td>issues.</td>
<td></td>
</tr>
<tr>
<td>Who will be</td>
<td>Head of IT</td>
</tr>
<tr>
<td>interviewed and</td>
<td>DP Officer</td>
</tr>
<tr>
<td>when?</td>
<td>Four developers.</td>
</tr>
<tr>
<td>What arrangements exist for personnel in</td>
<td>A group session at the start of the day and then individually as required.</td>
</tr>
<tr>
<td>case organisation to be briefed about the research and</td>
<td></td>
</tr>
<tr>
<td>their role?</td>
<td></td>
</tr>
<tr>
<td>What arrangements exist for case study personnel to read and sign the consent form?</td>
<td>All forms sent to site prior to visit with a request that the forms are read and signed ready for collection at the start of the interview.</td>
</tr>
<tr>
<td>How will transcripts</td>
<td>Final interview prompt covers this. Hopefully all will agree to read transcripts to check for accuracy and completeness.</td>
</tr>
<tr>
<td>be checked by</td>
<td></td>
</tr>
<tr>
<td>respondents?</td>
<td></td>
</tr>
</tbody>
</table>

**Documentation Control record for Case Study organisation**

<table>
<thead>
<tr>
<th>Interview with</th>
<th>Interview date</th>
<th>Date given for transcription</th>
<th>Back from transcription</th>
<th>Date sent for checking</th>
<th>Deadline date for changes and note of action needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of IT</td>
<td>20/10/04</td>
<td>27/10/04</td>
<td></td>
<td>16/1/05</td>
<td>30/1/05</td>
</tr>
<tr>
<td>DPO</td>
<td>13/10/04</td>
<td>19/10/04</td>
<td></td>
<td>3/2/05</td>
<td>17/2/05</td>
</tr>
<tr>
<td>Dev 1</td>
<td></td>
<td></td>
<td>Jan 05</td>
<td>16/1/05</td>
<td>30/1/05</td>
</tr>
<tr>
<td>Dev 2</td>
<td></td>
<td></td>
<td></td>
<td>16/1/05</td>
<td>30/1/05</td>
</tr>
<tr>
<td>Dev 3</td>
<td>20/10/04</td>
<td>27/10/04</td>
<td></td>
<td>24/1/05</td>
<td>6/2/05</td>
</tr>
<tr>
<td>Dev 4</td>
<td></td>
<td></td>
<td></td>
<td>24/1/05</td>
<td>6/2/05</td>
</tr>
</tbody>
</table>
### Site [ 3 ]:

<table>
<thead>
<tr>
<th>Name of site</th>
<th>A Unitary Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name and contact details of main contact.</strong></td>
<td>[Removed to provide anonymity for participating organisation]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is there a need for key respondents? If 'Yes':</th>
<th>Yes. [Name removed for anonymity] (Freedom of Information Project Leader) is the person through whom access was secured and he is acting as the link person for the organisation.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1: Has a briefing session been prepared?</strong></td>
<td>Yes, documents provided and distributed by him</td>
</tr>
<tr>
<td><strong>2: Has it been implemented?</strong></td>
<td>Yes, he has briefed all participants and arranged the day.</td>
</tr>
<tr>
<td><strong>3: Note emerging issues.</strong></td>
<td>Access to this organisation was given with some reluctance and this may be reflected in responses by participants in the research.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who will be interviewed and when?</th>
<th>DP Office</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Head of IT and E-Government</td>
</tr>
<tr>
<td></td>
<td>Two developers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What arrangements exist for personnel in case organisation to be briefed about the research and their role?</th>
<th>Briefed by the key respondent but offer briefing again at the start of each session.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Post event comment:</strong></td>
<td>Every one wanted briefing again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What arrangements exist for case study personnel to read and sign the consent form?</th>
<th>Distributed by key respondent and agreed that they would be collected at the start of each interview.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Post event comment:</strong></td>
<td>This didn’t happen. All respondents wanted reminding of the purpose of the research and time to read and sign the consent form at a later stage. It took some months to get all the consent forms signed and returned from this organisation. Note: the key respondent’s role was organisational; he did not contribute data to this study.</td>
</tr>
</tbody>
</table>

| How will transcripts be checked by respondents? | Final interview prompt covers this. Hopefully all will agree to read transcripts to check for accuracy and completeness. |

### Documentation Control record for Case Study organisation

<table>
<thead>
<tr>
<th>Interview with</th>
<th>Interview date</th>
<th>Date given for transcription</th>
<th>Back from transcription</th>
<th>Date sent for checking</th>
<th>Deadline date for changes and note of action needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of IT</td>
<td>1/11/04</td>
<td>15/11/04</td>
<td>Jan 05</td>
<td>5/2/05</td>
<td>19/2/05</td>
</tr>
<tr>
<td>DPO</td>
<td></td>
<td></td>
<td></td>
<td>13/1/05</td>
<td>27/1/05</td>
</tr>
<tr>
<td>Dev 1</td>
<td></td>
<td></td>
<td></td>
<td>24/1/05</td>
<td>6/2/05</td>
</tr>
<tr>
<td>Dev 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

192
## Interview prompts/questions for IS/IT Manager & DP Manager/Controller

<table>
<thead>
<tr>
<th>Prompt/Question</th>
<th>Res’ Notes</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introductions and seek permission to tape.</td>
<td>Verbally state these for audio recording</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>These can be recorded onto audiotape before the interview starts – less intrusive that way.</td>
<td></td>
</tr>
<tr>
<td>Case study organisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organisation code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff role</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff identity code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit of analysis being addressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tape code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transcription date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other notes about the session that may affect analysis?</td>
<td></td>
<td>Any other notes about the session can be added after the session is completed.</td>
</tr>
</tbody>
</table>

**Q 1** Check that consent form is understood. If not then explain the purpose of the interview – covering: nature of research, voluntary nature, confidentiality, check Consent Form signed and offer opportunity for respondent to ask questions/seek clarification. When explaining the nature of the research remain neutral and link to unit of analysis.

**Q 2** What is your role within the organisation? If Privacy and Data Protection not included – prompt: What about your role in relation to Privacy and Data Protection?

**Q 3** How long has Privacy and Data Protection been a feature of your work? Perhaps prompt – ‘is it reasonable’ or leave until Q16.

**Q 4** Tell me about any training or guidance in Privacy and Data Protection that you may have had?

**Q 5** Who else is involved in managing and providing for Privacy and Data Protection in the organisation? How does it all work together? Ie. How is it managed? Look for ethos, colleagues, management, etc.

193
| Q 6 | Is there a Privacy and Data Protection policy with regard to IS development and operation? IF YES - how was it developed and implemented? | Is there one for the organisation as a whole? |
| Q 7 | If not covered in Q 6 - Are a) you and b) your IS staff involved in formulating Privacy and Data Protection policies? | Seek follow-up regarding attitudes regarding ownership of policies and acceptance. |
| Q 8 | What is your role in informing IS systems practice with regard to Privacy and Data Protection? | Development and operation of systems. |
| Q 9 | How effective are your IS/IT staff in providing for Privacy and Data Protection? | Look for reasons and solutions. |
| Q 10 | How can their practice be improved? | Look for solutions. |
| Q 11 | It has been suggested that there are stages/activities in a development life cycle that offer greater opportunities for Privacy and Data Protection enhancements? In your opinion what stages/activities offer greatest potential for increasing Privacy and Data Protection? | Seek insights into why those stages. |
| Q 12 | Which IS/IT staff do you think have important contributions to make in providing for Privacy and Data Protection? | Why them and what in particular can they do? |
| Q 13 | Do you feel a responsibility to keep abreast of current legislation in the field of Privacy and Data Protection? |  |
| Q 14 | How easy is to keep up-to-date? |  |
| Q 15 | If Q14 negative - a) Please explain what barriers exist to restrict your ability to keep up-to-date. If Q14 positive – b) How do you keep up-to-date? |  |
| Q 16 | In your opinion is Privacy and Data Protection a legitimate concern of yours or should someone else be responsible for it? Who and why? | This question is left to the end so that ‘negative’ feelings are not encouraged at the start. |
| Q17 | Is there anything else in the area of Privacy and Data Protection that occurs in this organisation with regard to Privacy and Data Protection that you want to tell me about? Have I missed anything? |
| Q18 | Would you be prepared to read a transcript of this interview and confirm that my record is accurate?  
Can I email for queries that may arise? | Not necessary for the pilot study. |
| Q19 | Many thanks | Note ‘end time’ on tape. |
### Interview prompts & questions for IS developers

<table>
<thead>
<tr>
<th>Prompt/Question</th>
<th>Resp’</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introductions and seek permission to tape.</td>
<td>Verbally state these for audio recording</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case study organisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organisation code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff role</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff identity code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit of analysis being addressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tape code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transcription date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other notes about the session that may affect analysis?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admn’</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Check that consent form read and understood. If not then explain the purpose of the interview – covering: nature of research, voluntary nature, confidentiality, check Consent Form signed and offer opportunity for respondent to ask questions/seek clarification.</td>
</tr>
<tr>
<td>Q2</td>
<td>What does your job involve?</td>
</tr>
<tr>
<td>Q3</td>
<td>How long as Privacy and Data Protection been a feature of your work?</td>
</tr>
<tr>
<td>Q4</td>
<td>How is Privacy and Data Protection managed in the organisation? Who does what?</td>
</tr>
<tr>
<td>Q5</td>
<td>How do you personally know what’s expected of you with regard to Privacy and Data Protection?</td>
</tr>
<tr>
<td>Q6</td>
<td>Describe any guidance you have been given with regard to IS practice and need for Privacy and Data Protection</td>
</tr>
<tr>
<td>Q7</td>
<td>Do you feel that your knowledge of Privacy and Data Protection is sufficient to enable you to respond to its requirements effectively?</td>
</tr>
<tr>
<td>Q8</td>
<td>In your opinion is it reasonable to expect you to provide/consider Privacy and Data Protection – or should someone else be more involved?</td>
</tr>
<tr>
<td>Q9</td>
<td>In your opinion how should/can Privacy and Data Protection be built into info’ systems and processes?</td>
</tr>
<tr>
<td>Q10</td>
<td>How effective is the provision for Privacy and Data Protection in your development practice and in the organisation as a whole?</td>
</tr>
<tr>
<td>Q11</td>
<td>What can be done to make it more effective?</td>
</tr>
<tr>
<td>Q12</td>
<td>In your opinion are there particular stages in the development life cycle that offer significant potential for Privacy and Data Protection enhancements? What are these and what is the potential?</td>
</tr>
<tr>
<td>Q13</td>
<td>If some stages offer more potential than others – which staff have the greatest contribution to make and what is it?</td>
</tr>
<tr>
<td>Q14</td>
<td>Why do you address the issue of Privacy and Data Protection?</td>
</tr>
<tr>
<td>Q15</td>
<td>Describe the role of your IS management in the provision for Privacy and Data Protection?</td>
</tr>
<tr>
<td>Q16</td>
<td>What more can they do?</td>
</tr>
<tr>
<td>Q17</td>
<td>If you were the IS manager commissioned to produce systems that are Privacy and Data Protection compliant/sensitive – what would you do?</td>
</tr>
<tr>
<td>Q 18</td>
<td>Is there anything else in the area of Privacy and Data Protection that occurs in this organisation that you think I may like to know about? Have I missed anything?</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Q 19</td>
<td>Would you be prepared to read a transcript of this interview and confirm that my record is accurate? Can I email you if any need for clarification arises?</td>
</tr>
<tr>
<td>Q 20</td>
<td>Many thanks</td>
</tr>
<tr>
<td></td>
<td>Note ‘end time’ on tape.</td>
</tr>
</tbody>
</table>
Appendix 5: Survey Questionnaire

‘Survey of Information Systems professionals’ role in the provision for Privacy and Data Protection’

The purpose of this questionnaire is to determine the relationship between information systems staff and the increasing provision for privacy and data protection in organisations and within information systems. Your contribution will assist in the development of a set of guidelines for Information Systems staff so that they can produce and operate systems that are privacy sensitive. The research is being undertaken as part of a PhD programme of study and is supervised by staff from the Centre for Computing and Social Responsibility at De Montfort University, Leicester.

The questionnaire is intended to be completed by professionals, academics and students with experience in the area of information systems development.

Your responses are anonymous and will be treated in the strictest confidence. At no point during this research will any link be made between the responses provided and the contributor. It will be impossible to identify the source of any particular response. Should you wish to receive a copy of the survey outcome you can request this as described at the end of this questionnaire.

It should take no more than 10 minutes to complete the questionnaire and your contribution is appreciated. Thank you for your support and co-operation.

In making your responses please either place a '✓' in the corresponding box or circle your preferred response. If a question does not apply to you, please leave it and go on to the next one.

18 This is a copy of the postal questionnaire. The web-based questionnaire was identical in terms of questions asked but the format was slightly different to allow users to selected their responses using a mouse and click boxes.
Section A
General Perceptions Regarding Data Protection and Privacy

Questions 1 to 10 refer to your general perceptions regarding awareness of privacy and data protection issues in the information systems profession at large.

1. Information systems staff have a significant contribution to make in assisting organisations meet their obligations with regard to the 1998 Data Protection Act.

2. Awareness of the 1998 Data Protection Act amongst information systems staff is high.

3. I am aware of how the data protection principles affect the information systems development process.

4. I am aware of how the data protection principles affect the operation of information systems.

5. Data protection and data privacy is an increasing concern for information systems staff.

6. Involvement in privacy and data protection is a legitimate activity for information systems staff.

7. Organisations are providing suitable training in privacy and data protection issues for their employees.

8. Information systems professional associations, such as the BCS and IMIS, are providing appropriate guidance and advice for members regarding privacy and data protection issues.

9. In your view which three information systems jobs/roles provide the greatest opportunities to enhance privacy and data protection within information systems?

10. In your view which three stages in your systems development lifecycle provide the greatest opportunities to enhance privacy and data protection within information systems?
Section B
Involvement in Policy Formulation

The next section concerns involvement in privacy and data protection policy formulation and consultation.

11. Were you involved in any UK government or EEC consultation process regarding the development of data protection legislation?  
   Yes ☐  No ☐  
   (go to question 15)

12. Identify the type of involvement you had in the consultation process.  
   Please tick all that apply.  
   Individual response ☐  Response via your employer ☐  Response via professional body ☐  
   Other ☐  please specify ...

13. My involvement in the consultation process led to my greater acceptance of data protection legislation.

14. Involvement in the consultation process was a positive experience.

If you answered ‘No’ to question 11, please answer question 15, else go to question 16.

15. Identify the reasons for your lack of involvement in the consultation process.  
   I was not aware of the opportunity to contribute.  ☐  
   I was aware of the consultation process but decided not to contribute. ☐  
   Other ☐  please specify …
## Section C
### Data Protection and Privacy Policies

The following section is about privacy and data protection policies.

16. Does your organisation have a general privacy and or data protection policy for all employees?  
   - Yes □  
   - No □ (go to question 21)  
   - Don’t know □ (go to question 21)

<table>
<thead>
<tr>
<th>Question</th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Indifferent</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>17. I have a detailed knowledge of my organisations policy for all employees.</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>18. In my view the policy is understood by employees.</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>19. In my view the policy is applied by employees.</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>20. Information systems staff are involved in formulating and implementing privacy and data protection policies for all staff within my organisation.</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

21. Does your organisation have a privacy and or data protection policy specifically for Information Systems staff?  
   - Yes □  
   - No □ (go to question 26)  
   - Don’t know □ (go to question 26)

If you have answered ‘Yes’ to question 21, please answer questions 22 to 25 which relate to privacy and data protection policies for information systems staff, else go to question 26.

22. I have a detailed knowledge of my company’s policy for Information Systems staff.  
   - Strongly disagree □  
   - Disagree □  
   - Indifferent □  
   - Agree □  
   - Strongly agree □

23. In my view, my company’s policy is understood by information systems staff.  
   - Yes □  
   - No □ (go to question 26)  
   - Don’t know □ (go to question 26)

24. In my view, my company’s policy is applied by information systems staff.  
   - Yes □  
   - No □ (go to question 26)  
   - Don’t know □ (go to question 26)

25. Information systems staff are prominent in formulating and implementing privacy and data protection policies for information systems staff within my company.  
   - Yes □  
   - No □ (go to question 26)  
   - Don’t know □ (go to question 26)

26. Who is primarily responsible for privacy and data protection within your organisation?  
   Please identify one group only.

- An information systems member of staff □
- A dedicated Data Protection Official □
- Information systems staff and data protection staff in partnership □
- Other □ please specify ...

202
Finally, some questions about you that will assist in creating a profile of respondents. Please tick the appropriate response.

<table>
<thead>
<tr>
<th>Question</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>27. Which of the following job titles best describes your current position?</td>
<td>Manager/Director of Information Systems, Project Leader/Manager, Business Analyst, Systems Analyst, Database Manager/Administrator, Technical Services Manager, Other, please specify…</td>
</tr>
<tr>
<td>29. What is the total number of employees in your organisation?</td>
<td>Less than 10, 10-99, 100-499, 500-999, More than 1000, Other, please specify…</td>
</tr>
<tr>
<td>30. How long have you worked for this organisation?</td>
<td>Less than one year, 1-2 years, 3-4 years, 5-9 years, Over 10 years, Other, please specify…</td>
</tr>
<tr>
<td>31. How long have you worked in the Information Systems profession?</td>
<td>Less than one year, 1-5 years, 6-10 years, 11-20 years, Over 20 years, Other, please specify…</td>
</tr>
<tr>
<td>32. Is your age…</td>
<td>Under 25, Between 25-35, Between 36-45, Between 46-55, Over 56, Other, please specify…</td>
</tr>
<tr>
<td>33. In which country/location are you currently working?</td>
<td>Australia, Mauritius, Ghana, North America, Hong Kong, Singapore, India, South America, Rest of Europe, Sri Lanka, Malaysia, United Kingdom, Other, please specify…</td>
</tr>
</tbody>
</table>
If you answer ‘Yes’ to either of the next two questions your anonymity remains assured.

34. Would you like to receive a summary of the survey results? Yes ☐ No ☐

35. Would you consider supporting further research in the area of privacy and data protection? Yes ☐ No ☐

If you answer ‘Yes’ to either of questions 34 or 35 please email ccsr@dmu.ac.uk indicating which question[s] you answered ‘Yes’ to or include your name and address on a separate piece of paper and include it with the questionnaire when it is returned. Please be assured that no attempt will be made to link any questionnaire response with any individual or organisation.

Should you have any comments or questions regarding this research please contact the CCSR Web Master (ccsr@dmu.ac.uk), tel: 0116 250 6143 or Richard Howley, CCSR Research Associate (rgh@dmu.ac.uk), tel: 0116 207 8268.

Thank you for your contribution, it is greatly appreciated.

Richard Howley (Research Associate)
Center for Computing and Social Responsibility
De Montfort University
Leicester LE1 9BH
United Kingdom
Appendix 6: Covering letter to accompany the postal survey

Systems Development Manager
«Company»
«Address1» «Address2»
«Address3» «Address4»
«PostalCode»

5 September 2002

Dear Sir/Madam

Re: The role of computing staff in providing for privacy and data protection in systems development.

I regret addressing this letter in a non-personal manner, but please read-on. I am seeking your support for some important computing research that is currently being undertaken. The research is concerned with how systems developers design and build data protection and data privacy into systems and as a high quality provider of computer systems for businesses I specifically need input from companies such as yours. The result of the research, of which this questionnaire is one part, will be the production of a set of guidelines to assist computer professionals in developing systems that are more sensitive to privacy and data protection requirements. I hope that you can find 10 minutes of your time to assist in making this important research a success.

A copy of the questionnaire is enclosed and is also available online at: 
http://www.ccsr.cse.dmu.ac.uk/survey.

Whilst I would encourage you to return the completed questionnaire to me as soon as possible all responses received before the end of September 2002 will be used in the research. I enclose a pre-paid envelope for your reply.

All responses are totally anonymous, however, you may request a summary of the research findings as detailed at the end of the questionnaire. The summary of findings will be published by the end of October 2002.

If you have any questions about this research please do not hesitate to contact me. I do hope that you will contribute and thank you in anticipation.

Yours faithfully

Richard Howley
Research Associate (Centre for Computing & Social Responsibility)
School of Computing De Montfort University
Leicester LE1 9BH
Tel: 0116 207 8268
Email rgh@dmu.ac.uk
Appendix 7: Covering email to accompany the web based survey

----- Original Message -----
From: "Richard Howley" <rgh@dmu.ac.uk>
To: <DATA-PROTECTION@JISCMAIL.AC.UK>
Cc: "CCSR" <ccsr@dmu.ac.uk>; "Richard Howley" <rgh@dmu.ac.uk>
Sent: Tuesday, September 03, 2002 4:19 PM
Subject: Role of IS staff in developing systems for compliance

> Dear all,
>
> I am sending this mail to ask for your support - but, please read on. I am
> currently undertaking research as part of a PhD programme into Data
> Protection and Information Systems and am seeking professionals who are or
> who have been involved in the development of information systems (IS). The
> attached questionnaire takes about 10 minutes to complete, so if you are or
> have been involved in IS development and you can find 10 minutes to complete
> the questionnaire, I would be grateful. It can be completed and submitted
> online at: http://www.ccsr.cse.dmu.ac.uk/survey.
>
> If you would like a paper copy, please email me and I will send as many
> copies as you would like with pre-paid reply slips for your response.
>
> The results of the research are being written-up for presentation at a
> conference scheduled for the end of this year and if you would like to
> receive a copy of the research results the questionnaire does have a
> facility for you to request them. All contributions to the questionnaire are
> completely anonymous.
>
> Please, try to find time to complete the questionnaire and if you have
> colleagues that are involved in the IS development process, please consider
> forwarding this email to them so that they can contribute if they wish. The
> final part of the PhD will see the production of a set of IS development
> guidelines that will allow IS professionals to develop systems that are more
> sensitive to data privacy and protection. Clearly, this is important work
> and I hope that you can support it.
>
> Feel free to contact me if you have any questions or other contributions to
> make to this research.
>
> Regards and many thanks
> Richard Howley
> CCSR Research Associate & Principal Lecturer in IS
> Centre for Computing and Social Responsibility
> De Montfort University Leicester LE1 9BH
> email: rgh@dmu.ac.uk
> tel: +44 (0)116 255 551 fax: +44 (0)116 254 1891
> tel (mobile): 07951 084 593 http://www.cse.dmu.ac.uk/~rgh
Appendix 8: Survey data showing responses as percentages

Totals for WEB and paper Survey data with 59 responses:

<table>
<thead>
<tr>
<th></th>
<th>Totals as a %</th>
<th>Totals for 59</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Information systems staff have a significant contribution to make in assisting organisations meet their obligations with regard to the 1998 Data Protection Act.</td>
<td></td>
</tr>
<tr>
<td>Strongly Disagree</td>
<td>3.39</td>
<td>2</td>
</tr>
<tr>
<td>Disagree</td>
<td>3.39</td>
<td>2</td>
</tr>
<tr>
<td>Indifferent</td>
<td>1.69</td>
<td>1</td>
</tr>
<tr>
<td>Agree</td>
<td>44.07</td>
<td>26</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>47.46</td>
<td>28</td>
</tr>
<tr>
<td>Totals</td>
<td>100</td>
<td>59</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Awareness of the 1998 Data Protection Act amongst information systems staff is high.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Disagree</td>
<td>5.08</td>
</tr>
<tr>
<td>Disagree</td>
<td>45.76</td>
</tr>
<tr>
<td>Indifferent</td>
<td>18.64</td>
</tr>
<tr>
<td>Agree</td>
<td>28.81</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>1.69</td>
</tr>
<tr>
<td>Totals</td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>I am aware of how the data protection principles affect the information systems development process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Disagree</td>
<td>1.69</td>
</tr>
<tr>
<td>Disagree</td>
<td>6.78</td>
</tr>
<tr>
<td>Indifferent</td>
<td>8.47</td>
</tr>
<tr>
<td>Agree</td>
<td>66.10</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>16.95</td>
</tr>
<tr>
<td>Totals</td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>I am aware of how the data protection principles affect the operation of information systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Disagree</td>
<td>1.69</td>
</tr>
<tr>
<td>Disagree</td>
<td>6.78</td>
</tr>
<tr>
<td>Indifferent</td>
<td>13.56</td>
</tr>
<tr>
<td>Agree</td>
<td>59.32</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>18.64</td>
</tr>
<tr>
<td>Totals</td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Data protection and data privacy is an increasing concern for information systems staff.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Disagree</td>
<td>1.69</td>
</tr>
<tr>
<td>Disagree</td>
<td>3.39</td>
</tr>
<tr>
<td>Indifferent</td>
<td>10.17</td>
</tr>
<tr>
<td>Agree</td>
<td>49.15</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>35.59</td>
</tr>
<tr>
<td>Totals</td>
<td>100</td>
</tr>
</tbody>
</table>
Involvement in privacy and data protection is a legitimate activity for information systems staff.

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Indifferent</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disagree</td>
<td>1.69</td>
<td>3.39</td>
<td>47.46</td>
<td>47.46</td>
<td>1.69</td>
<td>100</td>
</tr>
<tr>
<td>Indifferent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

Organisations are providing suitable training in privacy and data protection issues for their employees.

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Indifferent</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Disagree</td>
<td>20.34</td>
<td>50.85</td>
<td>22.03</td>
<td>3.39</td>
<td>3.39</td>
<td>100</td>
</tr>
<tr>
<td>Disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indifferent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

Information systems professional associations, such as the BCS and IMIS, are providing appropriate guidance and advice for members regarding privacy and data protection issues.

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Indifferent</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Disagree</td>
<td>5.08</td>
<td>16.95</td>
<td>49.15</td>
<td>25.42</td>
<td>3.39</td>
<td>100</td>
</tr>
<tr>
<td>Disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indifferent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

Were you involved in any UK government or EEC consultation process regarding the development of data protection legislation?

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Indifferent</th>
<th>Disagree</th>
<th>Yes</th>
<th>No</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Disagree</td>
<td>91.53</td>
<td>8.47</td>
<td></td>
<td></td>
<td>91.53</td>
<td>8.47</td>
<td>100</td>
</tr>
<tr>
<td>Disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indifferent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Identify the type of involvement you had in the consultation process. Please click all that apply.

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Indifferent</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employer</td>
<td>16.67</td>
<td>33.33</td>
<td>50.00</td>
<td>1</td>
<td>1</td>
<td>100</td>
</tr>
<tr>
<td>Professional body</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

Identify the type of involvement you had in the consultation process. Please click all that apply.

Invited participant to Parliamentary Office of Science and Technology Electronic discussion as recognised specialist plus all listed options.

Attended working group and conference

Managed the work for CCTA when develop DP Guidelines
My involvement in the consultation process led to my greater acceptance of data protection legislation.

<table>
<thead>
<tr>
<th></th>
<th>Indifferent</th>
<th>Agree</th>
<th>Strongly Agree</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>58.82</td>
<td>23.53</td>
<td>17.65</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>4</td>
<td>3</td>
<td>17</td>
</tr>
</tbody>
</table>

Involvement in the consultation process was a positive experience

<table>
<thead>
<tr>
<th></th>
<th>Indifferent</th>
<th>Agree</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>55.56</td>
<td>44.44</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>8</td>
<td>18</td>
</tr>
</tbody>
</table>

Identify the reasons for your lack of involvement in the consultation process.

<table>
<thead>
<tr>
<th></th>
<th>Not Aware</th>
<th>Aware</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>88.00</td>
<td>12.00</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>6</td>
<td>50</td>
</tr>
</tbody>
</table>

Identify the reasons for your lack of involvement in the consultation process.

I was not working in this area at the time
Little chance to change things
Employer did not give opportunity to contribute.

Does your organisation have a general privacy and or data protection policy for all employees?

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Do not know</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>79.66</td>
<td>10.17</td>
<td>10.17</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>47</td>
<td>6</td>
<td>6</td>
<td>59</td>
</tr>
</tbody>
</table>

I have a detailed knowledge of my organisation's policy for all employees.

<table>
<thead>
<tr>
<th></th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Indifferent</th>
<th>Agree</th>
<th>Strongly Agree</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5.45</td>
<td>20.00</td>
<td>20.00</td>
<td>27.27</td>
<td>27.27</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>11</td>
<td>11</td>
<td>15</td>
<td>15</td>
<td>55</td>
</tr>
</tbody>
</table>

In my view the policy is understood by employees.

<table>
<thead>
<tr>
<th></th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Indifferent</th>
<th>Agree</th>
<th>Strongly Agree</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.91</td>
<td>29.09</td>
<td>23.64</td>
<td>32.73</td>
<td>3.64</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>16</td>
<td>13</td>
<td>18</td>
<td>2</td>
<td>55</td>
</tr>
<tr>
<td>Q20</td>
<td>In my view the policy is applied by employees.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strongly Disagree</td>
<td>Disagree</td>
<td>Indifferent</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td>Totals</td>
</tr>
<tr>
<td></td>
<td>5.45</td>
<td>27.27</td>
<td>27.27</td>
<td>30.91</td>
<td>9.09</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>15</td>
<td>15</td>
<td>17</td>
<td>5</td>
<td>55</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q21</th>
<th>Information systems staff are involved in formulating and implementing privacy and data protection policies for all staff within my organisation.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strongly Disagree</td>
</tr>
<tr>
<td></td>
<td>5.45</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q22</th>
<th>Does your organisation have a privacy and or data protection policy specifically for Information Systems staff?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Do not know</td>
</tr>
<tr>
<td></td>
<td>28.81</td>
</tr>
<tr>
<td></td>
<td>17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q23</th>
<th>I have a detailed knowledge of my company's policy for Information Systems staff.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strongly Disagree</td>
</tr>
<tr>
<td></td>
<td>6.67</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q24</th>
<th>In my view my company's policy is applied by information systems staff</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strongly Disagree</td>
</tr>
<tr>
<td></td>
<td>6.67</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
Information systems staff are prominent in formulating and implementing privacy and data protection policies for information systems staff within my company.

<table>
<thead>
<tr>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Indifferent</th>
<th>Agree</th>
<th>Strongly Agree</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.67</td>
<td>20.00</td>
<td>6.67</td>
<td>40.00</td>
<td>26.67</td>
<td>100</td>
</tr>
</tbody>
</table>

Who is primarily responsible for privacy and data protection within your organisation? Please identify one group only.

<table>
<thead>
<tr>
<th>IS Staff</th>
<th>Dedicated</th>
<th>Both</th>
<th>Other</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.31</td>
<td>13.79</td>
<td>24.14</td>
<td>32.76</td>
<td>100</td>
</tr>
</tbody>
</table>

Who is primarily responsible for privacy and data protection within your organisation? Please identify one group only.

- Individual Project Managers
- Commercial Director
- Head of site
- Not currently employed
- Information Officer within ICT, non technical member
- hr manager
- Don't know
- Don't know - think it is someone different in each university faculty
- Personnel Dept
- DP Official

Which of the following job titles best describes your current position?

<table>
<thead>
<tr>
<th>Student</th>
<th>Systems Analyst</th>
<th>sysprogrammer</th>
<th>Database Manager/Administrato</th>
<th>Other</th>
<th>Project Leader/Manager</th>
<th>Manager/Director of Information Systems</th>
<th>Network Manager/Administrator</th>
<th>Technical Services Manager</th>
<th>Business Analyst</th>
<th>Applications Programmer</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.08</td>
<td>6.78</td>
<td>6.78</td>
<td>3.39</td>
<td>22.03</td>
<td>20.34</td>
<td>16.95</td>
<td>1.69</td>
<td>3.39</td>
<td>3.39</td>
<td>10.17</td>
<td>100</td>
</tr>
</tbody>
</table>

Which of the following job titles best describes your current position?

- Data Officer
- Information Officer
- Clinical Systems specialist
- Project Co-ordinator
- Software Engineer
- Software Development Manager
- Test Analyst
- Head of Information
- Financial Analyst
- Implementation Consultant
- Legal Security Consultant
- Researcher
- Retired
- Administrator
<table>
<thead>
<tr>
<th>28</th>
<th>Which of the following best describes your organisation's business?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Public Sector</td>
</tr>
<tr>
<td></td>
<td>Academic</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<tr>
<td></td>
<td>Private Enterprise: Computer Industry</td>
</tr>
<tr>
<td></td>
<td>Self-Employed/Contractor</td>
</tr>
<tr>
<td></td>
<td>Private Enterprise: Non-Computing Industry</td>
</tr>
<tr>
<td></td>
<td>Totals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>28</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RSL</td>
</tr>
<tr>
<td></td>
<td>Utilities</td>
</tr>
<tr>
<td></td>
<td>Financial Sector</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>29</th>
<th>What is the total number of employees in your organisation?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Less than 10</td>
</tr>
<tr>
<td></td>
<td>10-99</td>
</tr>
<tr>
<td></td>
<td>100-499</td>
</tr>
<tr>
<td></td>
<td>500-999</td>
</tr>
<tr>
<td></td>
<td>More than 1000</td>
</tr>
<tr>
<td></td>
<td>Totals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>30</th>
<th>How long have you worked for this organisation?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Less than one year</td>
</tr>
<tr>
<td></td>
<td>1-2 years</td>
</tr>
<tr>
<td></td>
<td>3-4 years</td>
</tr>
<tr>
<td></td>
<td>5-9 Years</td>
</tr>
<tr>
<td></td>
<td>Over 10 years</td>
</tr>
<tr>
<td></td>
<td>Totals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>31</th>
<th>How long have you worked in the Information Systems profession?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Less than one year</td>
</tr>
<tr>
<td></td>
<td>1-5 years</td>
</tr>
<tr>
<td></td>
<td>6-10 years</td>
</tr>
<tr>
<td></td>
<td>11-20 years</td>
</tr>
<tr>
<td></td>
<td>Over 20 years</td>
</tr>
<tr>
<td></td>
<td>Totals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>32</th>
<th>Is your age...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Under 25</td>
</tr>
<tr>
<td></td>
<td>Between 25-35</td>
</tr>
<tr>
<td></td>
<td>Between 36-45</td>
</tr>
<tr>
<td></td>
<td>Between 46-55</td>
</tr>
<tr>
<td></td>
<td>Over 56</td>
</tr>
<tr>
<td></td>
<td>Totals</td>
</tr>
</tbody>
</table>
### 33 In which country/location are you currently working?

<table>
<thead>
<tr>
<th>Location</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>3.39</td>
<td>2</td>
</tr>
<tr>
<td>USA</td>
<td>1.69</td>
<td>1</td>
</tr>
<tr>
<td>Singapore</td>
<td>1.69</td>
<td>1</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>93.22</td>
<td>55</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>100</td>
<td>59</td>
</tr>
</tbody>
</table>

### 34 Would you like to receive a summary of the survey results?

<table>
<thead>
<tr>
<th>Response</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>30.51</td>
<td>18</td>
</tr>
<tr>
<td>Yes</td>
<td>69.49</td>
<td>41</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>100</td>
<td>59</td>
</tr>
</tbody>
</table>

### 35 Would you consider supporting further research in the area of privacy and data protection?

<table>
<thead>
<tr>
<th>Response</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>31.03</td>
<td>18</td>
</tr>
<tr>
<td>Yes</td>
<td>68.97</td>
<td>40</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>100</td>
<td>58</td>
</tr>
</tbody>
</table>
In your view which three information systems jobs/roles provide the greatest opportunities to enhance privacy and data protection within information systems?

- Data Protection Officer role
- IT manager
- DBA

Network manager Database admin User support
project manager systems analyst Network Manager
Systems Analysts, Systems Developers, Database Managers.
MIS Manager Developer DBA
Data Protection Managers IT Security technicians Internal Auditing
Chief Information Officer Systems Analyst
Systems Manager Network Manager Applications manager
Database administrators Systems developers Website developers/managers
DBA System Developer Systems Analyst
Unable to comment usefully I'm afraid!
Head of IT, Project manager, User representative
Development manager Network manager Organiser of BackUp Procedure
Application Development. Support and Training. Systems Administration
IT Manager, Service Delivery Manager, Information/data protection officer
System Developers, System / Network Administrators, IT Managers
IT Consultants, Systems Architects and Project Managers
System administrators Business Analysis and System Design All top management
1. Head of Department (influence at Board level) 2. Business Analyst (legal requirements, best practice
Database Development Systems Administrators Systems Analysts
Systems Developer Network security manager IT/IS Manager
IS Senior Management Network and Security Manager Training Manager
System Analyst System Programmer Database Administrator
DBA System Manager Test manager
Data officer IS Administrator Marketing
A specific IS Security Officer role- Project manager of systems development with further responsibility for operational implementation
System Analyst, Programmer and tester
systems analysts IT Manager programmer
IS Management - it must be led from the top Business Analyst Database Administrator
Developers Systems analysts IT Managers/Data Protection Officer
IT Manager Technical Architect Systems Desinger
project manager business analyst manager
Project Manager Systems Analyst Team Leader
IT Manager, Director level position, security officer
IS Manager Database Administrator Internet/Intranet Administrator
Functional designer Technical designer/architect System administrator
project manager- programmers - systems security
IT Director, Systems Architect, Business Analyst/Consultant
MIS Manager PM DBA
System Sponsor (Because the developer will generally have to comply with the sponsors stated or documented requirements.) System
Administrator System User
network security staff 2) programmers writing security permissions into their front end systems 3) dba ensuring permissions
are adequate on databases.
Data Protection Officer Project Leaders / Designers Database Managers
Business analyst Systems analyst Systems designer
Network Administrator
IT Administrator - Systems programmer/Developer - CEO
PM's - analysts - change control managers
Executive sponsor - PM - Technical Design Authority
IS manager - PM - Designer
Design- management - end-user
Systems analyst - DBA - Network Admin
In your view which three stages in your systems development lifecycle provide the greatest opportunities to enhance privacy and data protection within information systems?

- specification of new system - revamping or modifying existing systems - Audits
- Initial planning Permissions set-up User training
- Analysis, design and implementation
- Requirement gathering Analysis early design
- Continuous
- Project Definition Project Proof of Concepts Project Review
- Specification Development
- Design UAT
- Fact Finding stage (i.e. what data are we going to collect?) Design stage Implementation stage
- Design Implementation Testing
- Ditto!
- Initial investigation and specification
- Database security Network security Training of staff in use of software
- Planning, Planning, Planning.
- Consultation with workstream leaders - highlights awareness & can lead to initial concept being redrafted. Training and role out of systems.
- Analysis, Design and Testing
- Bid Stage, systems design and implementation
- Initial requirements analysis including feasibility study Interface design strategy During the design planning with processes and codes.
- 1. Feasibility study 2. Requirements gathering
- Design Design Design
- Requirements analysis design testing (Ethical Hacking)
- Requirements gathering Design Specification Implementation & Training
- High level design Technical specification System test
- Design Code Test
- Research Implementation Testi

Don't understand the question. My experience is with phased developments and implementation.

Good privacy practise and data protection should be specified at the requirements/scoping phase of system development and the design, implementation and operational should be built into the whole process feasibility study analysis design
- Business Process Design Data analysis/design System logical design
- All stages
- Functional Specification Systems Design Systems Implementation
- Discovery design specification
- Analysis Development Testing
- Every stage
- Functional design Technical design Deployment planning
- Planning testing implementation
- Requirements Analysis, Database Design, Prototyping/User Acceptance Testing
- Early input and ongoing
- Specification Acceptance Implementation
- 1) initial discussions with users - tiered access 2) designing front end validation 3) designing data objects
- Inception Design Implementation

Initial Planning
- Systems Design - Systems Security Set-up - Data distribution design
- Inception/definition - analysis - review/control
- Proj initiation - Implementation - Operational support
- Systems Design - implementation - training/handover
- Specification/Design - Implementation - user testing
- Planning - implementation - development
- Conception/planning - analysis - design

215
Appendix 9: Summary of the survey data

The role of IS staff in the provision for privacy and data protection
© Richard Howley 2002 (rgh@dmu.ac.uk)

Question 1:
Information systems staff have a significant contribution to make in assisting organisations meet their obligations with regard to the 1998 Data Protection Act.

Question 2:
Awareness of the 1998 Data Protection Act amongst information systems staff is high.
Question 3:
I am aware of how the data protection principles affect the information systems development process.

Question 4:
I am aware of how the data protection principles affect the operation of information systems.

Question 5:
Data protection and data privacy is an increasing concern for information systems staff.
Question 6:
Involvement in privacy and data protection is a legitimate activity for information systems staff.

Question 7:
Organisations are providing suitable training in privacy and data protection issues for their employees.

Question 8:
Information systems professional associations, such as the BCS and IMIS, are providing appropriate guidance and advice for members regarding privacy and data protection issues.
**Question 9:** In your view which three information systems jobs/roles provide the greatest opportunities to enhance privacy and data protection within information systems?

<table>
<thead>
<tr>
<th>IS Role</th>
<th>No' identifying role</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT/MIS/Systems Manager</td>
<td>28</td>
</tr>
<tr>
<td>Systems Analyst</td>
<td>19</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>12</td>
</tr>
<tr>
<td>Systems Developers</td>
<td>11</td>
</tr>
<tr>
<td>Systems Designer</td>
<td>9</td>
</tr>
<tr>
<td>Systems Administrators</td>
<td>7</td>
</tr>
<tr>
<td>Project Manager</td>
<td>7</td>
</tr>
<tr>
<td>Network Manager</td>
<td>6</td>
</tr>
<tr>
<td>IT Security Personnel</td>
<td>6</td>
</tr>
<tr>
<td>Programmers</td>
<td>6</td>
</tr>
<tr>
<td>Data protection Official</td>
<td>5</td>
</tr>
<tr>
<td>Support and Training</td>
<td>4</td>
</tr>
</tbody>
</table>

**Question 10:** In your view which three stages in your systems development lifecycle provide the greatest opportunities to enhance privacy and data protection within information systems?

<table>
<thead>
<tr>
<th>Stage</th>
<th>No' identifying stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Design</td>
<td>35</td>
</tr>
<tr>
<td>Systems Analysis</td>
<td>21</td>
</tr>
<tr>
<td>Implementation</td>
<td>17</td>
</tr>
<tr>
<td>Project Initiation and Planning</td>
<td>13</td>
</tr>
<tr>
<td>Testing</td>
<td>10</td>
</tr>
<tr>
<td>Training users</td>
<td>5</td>
</tr>
<tr>
<td>Embed in the whole process</td>
<td>5</td>
</tr>
<tr>
<td>Coding/Programming</td>
<td>4</td>
</tr>
<tr>
<td>Feasibility study</td>
<td>3</td>
</tr>
</tbody>
</table>

**Question 11:** Were you involved in any UK government or EEC consultation process regarding the development of data protection legislation?

![Bar Chart](Q11.png)
Question 12:
Information systems professional associations, such as the BCS and IMIS, are providing appropriate guidance and advice for members regarding privacy and data protection issues.

Question 13:
My involvement in the consultation process led to my greater acceptance of data protection legislation.

Question 14:
Involvement in the consultation process was a positive experience.
Question 15: Identify the reasons for your lack of involvement in the consultation process.

Question 16: Does your organisation have a general privacy and or data protection policy for all employees?

Question 17: I have a detailed knowledge of my organisation's policy for all employees.
Question 18: In my view the policy is understood by employees.

Question 19: In my view the policy is applied by employees.

Question 20: Information systems staff are involved in formulating and implementing privacy and data protection policies for all staff within my organisation.
Question 21:
Does your organisation have a privacy and/or data protection policy specifically for Information Systems staff?

Question 22:
I have a detailed knowledge of my company's policy for Information Systems staff.

Question 23:
In my view my company's policy is understood by information systems staff.
Question 24:
In my view my company's 60 policy is applied by information systems staff 50

---

Question 25:
Information systems staff are prominent in formulating and implementing privacy and data protection policies for information systems staff within my company.

---

Question 26:
Who is primarily responsible for privacy and data protection within your organisation? Please identify one group only.
Question 27:
Which of the following job titles best describes your current position?

Question 28:
Which of the following best describes your organisation's business?

© Richard Howley 2002
De Montfort University
Leicester
LE1 9BH
rgh@dmu.ac.uk
### Appendix 10: Criteria for selecting industry sector for inclusion in the case study research

<table>
<thead>
<tr>
<th>Feature</th>
<th>Local Authorities</th>
<th>General Manufacturing</th>
<th>Financial Services</th>
<th>Software Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do cases provide a large amount of personal data handling?</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Do formal quality standards exist?</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Are cases likely to share a sense of responsibility for PDP?</td>
<td>✓</td>
<td>Not known</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Is there homogeneity of like cases/population?</td>
<td>✓ (evidence does exist to question this)</td>
<td>✓ (within sectors)</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Is there a high degree of external regulation?</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Are there a large number of data subjects?</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Do cases have similar number of IS/IT staff?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Do cases develop IS?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Do cases maintain IS?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Do cases manage the operation of IS?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Do sector Code of Practice exist to guide IS practice?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Is confidentiality a recognised important issue for cases?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Is the IS/IT function small enough for 3/4 respondents to represent the views of the organisation</td>
<td>✓</td>
<td>✓ (some)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Is there an organisational Policy for PDP?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Is sensitive data likely to be present?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Appendix 11: Letter sent to potential case study organisations

Address and date

Dear ...........

I am writing to seek your support for research being undertaken by staff from the Centre for Computing and Social Responsibility (CCSR) at De Montfort University, Leicester. The research is concerned with:

1. the impact recent legislation (in the field of privacy and data protection) is having on the pattern of systems development practice, and
2. the way organisations manage their systems development processes in the light of an increasing need to comply with privacy and data protection legislation.

As with all research of this kind confidentiality regarding your business affairs is assured (see the attached Consent Form for further details).

We want to gather data from UK Local Authorities that employ systems/business analysts or systems developers. It is hoped that this research will take place during September and October 2004. The extent of your involvement can be as large or small as you wish, but as minimum we would hope to conduct interviews with those responsible for managing the systems development process and the person responsible for data protection. The research also requires that we interview some or all of your development staff. It is anticipated that these interviews will last approximately 45 minutes. Details of the questions to be asked are available for your review on the research web-site (see http://www.cse.dmu.ac.uk/~rgh/pdp-research). In conducting this research we assure you that we will seek to be as unobtrusive as possible.

I do hope that you will be prepared to support this research. By sharing your insights and expertise with the wider IS community you will be contributing significantly to the development of information systems practice within the UK. Attached, for your information, is a ‘Frequently Asked Questions’ sheet and a Consent Form that will be distributed to all potential participants in this research. These provide further information regarding this research and as such they may answer any questions that you have. However, if you do have any further questions about this research that you wish to discuss, please do not hesitate to contact me on 0116 207 8268 or by email rgh@dmu.ac.uk. For further information about CCSR see http://www.ccsr.cse.dmu.ac.uk/.

If you want to ask any further questions regarding the research before committing yourself to take part please do not hesitate to contact me, otherwise I will contact you early next week to discuss this research. If you feel that this letter has been sent to the wrong person in your organisation, please pass it to the appropriate person so that they may consider participating. The letter has been sent to the person responsible for Data Protection and the Head of IT/IS Manager within your organisation.

Whether you decide that you can support this research or not, I appreciate your consideration of this matter.

Yours faithfully,

Richard Howley, Principal Lecturer in Information Systems & Research Associate in the Centre for Computing and Social Responsibility
Appendix 12: ‘Frequently Asked Questions (FAQs)’ document sent to potential case study organisations

Privacy and Data Protection Research
Centre for Computing & Social Responsibility
De Montfort University - Leicester

FAQ’s

Who is the lead researcher?
Richard Howley Principal Lecturer in Information Systems & Research Associate, Centre for Computing and Social Responsibility
De Montfort University, Leicester.

What is the research about?
The research is part of an ongoing research project into the role of Information Systems staff in providing Privacy and or Data Protection.

How much time will be required?
Between 45 minutes and 2 hours, your contribution will be as much or little as you agree to.

What about confidentiality?
Confidentiality will be maintained. Any comments made and recorded will be kept secure and destroyed as soon as is practicable. We would hope, with your agreement, to identify organisations that contributed to the research in order that our appreciation can be publicly expressed.

Will anyone know what I say?
No. No individual will be identified unless they agree and provide written approval for their comments to be attributed to them.

What will happen to the notes the researcher makes?
These will be kept in secure storage for as long as they are required for data analysis purposes. Once this stage of the research is completed, and in any event by the end of 2005, they will be shredded or incinerated.

Will my employer know what I said?
No. The findings will be presented in a way that guarantees anonymity for all individual contributors unless they agree and provide written approval for their comments to be attributed to them.

Can I see the results of the search?
Yes. The findings will be made available to all contributing organisations and individuals. It is anticipated that the results will also be published in an academic journal and or conference proceedings.
Why should I take part?

The CCSR will be using the results of this research to inform its representations of the profession to the UK Government and the Information Commissioner. It is important that your voice is heard.

Can I withdraw from the research?

Yes. At any point you can request to withdraw from the research and any data provided by you will be promptly destroyed.

Do I need to know about privacy and data protection to take part?

No. We are not seeking ‘experts’ in the field, though they would be very welcome, if they are out there. Rather we hope to seek the views of development staff and their managers that have considered or who are prepared to consider how best to meet the privacy and data protection challenge in IS professional practice.

Can I ask questions before deciding?

Contact Richard Howley: Tel: 0116 207 8268 or Email: rgh@dmu.ac.uk
Appendix 13: Conference paper presented at ETHICOMP 2002 Universidade Lusiada, Lisbon, Portugal November 2002


Abstract

This paper addresses the changing role of information systems (IS) staff in the provision for privacy and data protection (PDP) in organisations and within information systems. A literature review is reported on which identifies the contribution that IS professionals are believed to be able to make in the provision for PDP. Significant amongst these are the use of PDP design strategies and the application of privacy enhancing technologies. The findings of a survey of IS staff is then presented. The survey explored the attitudes and roles that IS staff have with regard to their involvement in the provision for PDP. It is shown that whilst IS staff are supportive of involvement in the provision for PDP they regard the role of both IS and business managers as important factor in the overall provision. Aspects of IS professional practice and IS roles are identified as offering particular opportunities for PDP leverage. However, there are many issues in the complex PDP matrix that need to be addressed before IS staff can contribute fully. These are identified and discussed. The paper concludes by acknowledging that IS staff alone cannot provide PDP within organisations; it has to be a collaborative approach within an environment that is sensitive to and supportive of PDP.

1. Introduction

Many societies throughout the world are currently designing or implementing national schemes for privacy and data protection (PDP). The European provision for PDP is seen by many as a model to follow and or emulate (Ross 2001). It is argued here that in order to provide for effective PDP, organisations will need to transform the way they manage the systems development process, analyse data requirements, design and operate information systems (IS). Fundamental to this process is the role of the IS professional. This paper reports the findings of on-going research into the relationship between IS staff and the provision for PDP.

This paper will firstly outline the research rationale and identify several research questions that emerge. Following this a consideration of the methods used to address these research questions is offered along with a brief overview of the respondent profile. Each of the research questions are then addressed in the light of the emerging
research data. The paper concludes by considering future research issues that arise from the discussion and findings.

2. Research Rationale

This research originated due to an increasing awareness of the need for data privacy and protection within organisations and information systems. Since the publication of the Draft General Directive on ‘the protection of individuals with regard to the processing of personal data and at the free movement of such data’ by the European Commission in September 1990 (Directive 95/45/EC) the role of the IS professional has been increasingly identified as an important factor in the provision for data privacy and protection. Whilst this process was taking place it became an increasing concern of the authors that ‘rank and file’ systems developers did not appear to be engaged in either;

the consultation process that accompanied the development of PDP legislation, or
in the apparent ‘role-adjustment’ that appeared to be taking place.

This concern led to the development of several research questions some of which are reported upon in this paper. The research questions addressed in this paper are:

1. What is the emerging role for IS staff in supporting the provision of PDP?
2. Which IS staff and what systems development activities present PDP enhancing opportunities?
3. Are IS staff equipped to meet the challenges of their new role?

It is felt that if IS staff are new custodians of data privacy and protection then the degree to which they are aware of and accepting of this responsibility will be critical in determining whether data is adequately protected or not. Before reporting the research findings in relation to these questions it is first necessary to outline the methods used in the research and provide some details of the respondent group from which conclusions are drawn.

3. Methods and respondent profile

3.1 Research Methods

The findings reported in this paper are one part of a PhD programme of study involving different approaches and methods. A literature review was undertaken to explore the evolving role of IS staff in relation to PDP and its legislative framework.

In addressing which IS staff and what systems development activities present PDP enhancing opportunities a survey of IS staff was designed and undertaken. Thomas (1996, p115) regards questionnaires as useful in ‘estimating relationships between
variables’ and as this survey explicitly seeks to do this it is seen the most appropriate method. The survey sought the views of IS staff with regard to their role in the provision for PDP. The survey also sought the views of IS staff with regard to which staff can contribute and at what stage of the systems development process. The research is specifically aimed at discovering actual levels of awareness, attitudes to PDP provision and about how PDP is provided for within organisations. This is achieved through the use of open and closed questions providing qualitative and quantitative data.

The research sample was drawn from the whole of the UK and consists of a relatively large number of respondents. Not all responses were required to enable conclusions to be drawn from the data.

The questionnaire was piloted prior to distribution. Piloting tested that the questionnaire was meaningful and understandable to the respondents and secondly, to assure that the results would be suitable for extracting appropriate research data. Interviews with a sub-set of the pilot group took place to further assure the appropriateness of the questionnaire and to get meaningful respondent feedback. The piloting and interviews led to further refinement of the questionnaire before it was distributed to the full respondents set.

3.2 Respondent Profile

The questionnaire was sent to:

4. A Data Protection mail list that includes some IS professionals.
5. Thirty alumni of postgraduate computing programmes.
6. Ninety large and small companies all of whom claim to provide a complete systems development service. Companies were selected paying due regard to geographical location.

Forty two usable responses have been received at the time of writing and before considering the actual data it is worth providing a brief summary of the respondent profile. The questionnaire included a section that collected data regarding the nature of the respondent group. This was done to allow for an assessment of representativeness to occur. The two largest professional group represented in the respondent set are Project Managers and Managers/Directors of Information. Together they accounted for more than one third of all respondents. The next largest group accounting for 10% of responses was Network Managers, which was followed by Technical Services Managers with 5 % of returns. Overall, managers accounted for more than half of all responses and this has implications for the validity of the finding and future research. The respondent group are an experienced body of IS professionals. Forty five percent of respondents have worked in the IS profession for between one and five years whilst a further 43% have been in the profession for more than six years.

Sixty percent of responses came from personnel working in large (more than 1000 employees) organisations with a further 10% working in organisations with between 500 and 999 employees. It may be that personnel working in smaller companies may
have a different view of PDP. With regard to economic sector the following profile emerged:

<table>
<thead>
<tr>
<th>Economic Sector</th>
<th>Respondents as a %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Enterprise: Computing</td>
<td>31%</td>
</tr>
<tr>
<td>Public Sector</td>
<td>24%</td>
</tr>
<tr>
<td>Private Enterprise: Non-Computing</td>
<td>19%</td>
</tr>
<tr>
<td>Academic</td>
<td>14%</td>
</tr>
<tr>
<td>Other</td>
<td>7%</td>
</tr>
<tr>
<td>Self Employer/Contractors</td>
<td>5%</td>
</tr>
</tbody>
</table>

Sample design sought to target sufficient respondents to allow for a representative sample to emerge. Actual respondents are experienced IS professionals that are representative of the IS profession, in wide range of organisations of different sizes. It is suggested that the profile presented allows for valid judgements to be made with regard to reporting progress in this research. Follow-up work will seek to include a larger number of smaller companies and more non-management personnel in the respondent set.

4. What is the emerging role for IS staff in supporting the provision of PDP?

4.1 Literature review findings

The literature review found evidence that IS staff are increasingly seen as providers of data privacy and protection in organisations and within systems practice and it to a consideration of those finding that we now turn.

With regard to role of IS staff a considerable amount of literature exists that supports their involvement in the provision for PDP. Principle seven of the 1998 Data Protection Act (DPA) requires organisations to have due regard to the technical protection of privacy and data. Given the skills and expertise of IS personnel it is they that have the responsibility for providing this ‘due regard’. The Information Commissioner (ODPR, 1997; France, 2000) develops this further by referring to:

1. The need to embed PDP into the design of information systems.
2. The emergence of an ‘ethical engineer’ applying ‘privacy enhancing technologies’.
3. A merging of roles between IS staff and others in the PDP environment with responsibilities with regard to data.

The contribution of IS staff has also been considered in relation to other legislation that has emerged since the 1998 Data Protection Act. In the introduction to the Freedom of Information Act 2000, the Information Commissioner (IC) states that organisations will not be able to ‘determine their publications schemes if the presence
and structure of data is not known’ (OIC 2001). Clearly, IS staff are instrumental in structuring and providing access to an organisation's data resources.

As well as identifying the involvement of IS staff in the provision for PDP their relationships with other organisational staff has received attention. Lycett and Pouloudi (1999) considered ‘issues of data protection in contemporary development environments’ highlighting the ‘complex ethical debate for data controllers,..., the supervisory authority that oversees data protections, and information systems developers’. With regard to the then imminent enactment of the 1998 Act the Data Protection Registrar (as the office was known as at that time) states that “IT managers will have to work with other divisions, such as marketing, finance and personnel to make this [work] ... Data Protection is not just about IT – they cannot be successful by themselves” (France 2000). IS staff then not only have a contribution to make as a profession they are also required to collaborate with other professionals in the complex and evolving provision for PDP.

The role of IS staff is often referred to in a general manner in relation to supporting PDP. In recent years however, attention has focussed on the use of Privacy Enabling Technologies (PETs) and the importance of systems design. The IC has been active in promoting the view that PDP can be facilitated through the application of PETs in systems design and operation (ODPR 1997?). It is claimed that PETs are not regarded as novel or highly complex; physical controls and software design can significantly enhance PDP. Rabb (1999) add that PETs are not just a technical fix that can be applied retrospectively, but should be applied as a fundamental part of the design process. The role of IS staff in applying PETs through ‘compliant design’ is increasingly seen as a key to data privacy and protection.

With regard to the opportunities systems design offers PDP the IC has stated that ‘conventional IS can be transformed to have a privacy-enhancing effect if they are designed in the right way’. The IC is promoting the view that a systems design philosophy can significantly enhance the protection of individual privacy (France 2000). In the same article she refers to ‘privacy friendly IS design’ and the role of the ‘ethical engineer’ in facilitating compliant software and systems. Rabb (1999) states that “those that design the systems and services with which they work are increasingly important as participants in the system’ for PDP. He is suggesting that the role of IS staff is critical in building into systems the provision for compliance with existing legislation and the flexibility to better meet the changing and unknown requirements of further legislation. Rabb goes on to report that the ‘UK DPR has discussed privacy issues with ...[various large systems providers and] ... invited providers to design privacy into systems and for them to be part of the solution rather than the problem’ (Rabb 1999). To support this process further the OIC has commissioned research to investigate the extent to which UK based websites comply with the terms of the 1998 Data Protection Act (IC 2002). Further research commissioned by the OIC has resulted in a consultation document being published that examines the contribution systems designers can make in the provision for PDP (ODPR 2000, Watts and Macaulay 2002).
With regard to E-commerce start-ups, but applicable to all systems development, the lead article of ‘Privacy and Data Protection’ (October 2000, p1) states that “it is important for E-commerce start-ups to be aware of data protection legislation at the time when the website is created. Developing compliance after the site has been up and running may involve expensive changes that many [all] start-ups can ill afford”. Clearly, IS staff are the ones that carry the responsibility for creating these ‘start-ups’ and as such they need to be aware of the PDP requirements, privacy enabling technologies and strategies that can be employed and applied.

Members of the IS profession readily accept the responsibility to design for compliance. The IMIS Survey 2002 (Prior, Fairweather and Rogerson 2002) found that 90% of respondents agreed with the statement that ‘IS staff should design systems for PDP compliance’. Furthermore, evidence presented later in this paper regarding the role of IS staff supports the IMIS findings. Systems design is therefore seen, as a key activity in the provision for PDP and this is readily accepted by IS staff.

PDP is closely related to data security and it is no surprise to find that research into computer security has considered data protection and privacy. Anton and Earp (2000) conclude their study of requirements for secure ECommerce systems by stating that ‘data protection has regrettably subsisted as an afterthought when designing new systems; however, it is becoming a critical development concern’. Hes and Borking (1998) show how IS staff can contribute to data privacy and protection by ‘anonymising data’ through the use of ‘personal identifiers’.

The literature review concluded that there is a growing awareness that we must have proactive ‘design for privacy’ and not a reactive ‘fix for compliance’ and that the application of PET’s, systems design and systems security are clear IS responsibilities.

4.2 Questionnaire data and the role of IS staff

Having identified the role of IS staff as defined in the literature we can now turn our attention to the role as perceived by members of the IS profession. The research undertaken found that considerable support for the involvement of IS staff in the provision for PDP. Ninety three percent of respondents believe that IS staff have a significant contribution to make in assisting organisations meet their PDP obligations. Moreover, 95% report that PDP is a legitimate activity for IS staff to be involved with and 81% felt that it is an increasing concern for IS professionals. Indeed, for many IS professionals the provision for PDP may now be a major part of their professional life. IS staff are active in determining and implementing the PDP policies within organisations. It was reported that in 26% of organisations IS staff have primary responsibility for PDP and in 24% PDP is a shared responsibility between IS staff and DP officials.

These findings confirm the view that IS staff have an important role to play in the provision for and management of PDP and that this role is seen as legitimate by member of the profession.
5. Which IS staff and what activities present PDP enhancing opportunities?

As stated earlier the role of IS staff in the provision for PDP is a relatively recent development and it may be a consequence of this that the precise nature of that role is presented in a general rather than specific manner. This gave rise to the second research questions addressed in this paper, ‘which IS staff and what IS activities present PDP opportunities?’.

Two questions on the survey specifically addressed these issues, they were:

In your view which three information systems jobs/roles provide the greatest opportunities to enhance privacy and data protection within information systems?

In your view which three stages in your systems development life cycle provide the greatest opportunities to enhance privacy and data protection within information systems?

Table 1 presents the responses to the first of these two questions:

<table>
<thead>
<tr>
<th>IS Role</th>
<th>Number of respondents identifying role</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT/MIS/Systems Manager</td>
<td>23</td>
</tr>
<tr>
<td>Systems Analyst</td>
<td>15</td>
</tr>
<tr>
<td>Systems Developers</td>
<td>9</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>9</td>
</tr>
<tr>
<td>Network Manager</td>
<td>6</td>
</tr>
<tr>
<td>Systems Administrators</td>
<td>6</td>
</tr>
<tr>
<td>Project Manager</td>
<td>7</td>
</tr>
<tr>
<td>Programmers</td>
<td>3</td>
</tr>
<tr>
<td>IT Security Personnel</td>
<td>5</td>
</tr>
<tr>
<td>Systems Designer</td>
<td>3</td>
</tr>
<tr>
<td>Support and Training</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 1: IS roles in the provision for PDP

A notable feature of the data presented in Table 1 is the identification of managers as key providers in the provision for PDP. Some respondents felt so strongly about this they annotated their response with emphasis on role of senior management. In the literature review the role of managers in facilitating PDP within the IS profession and within systems was not prominent. It may be that the emphasis on PETs and systems design may be lead to a neglect of the important role of [senior] management in the provision for PDP. The role of systems designer is not as significant in the data as one may expect given the prominence they have in the literature. The reasons for this are to be explored further and reported upon at a later date.

Stages in the systems development process that were identified by IS staff as offering opportunities for PDP leverage are presented in table 2:
Stage | Number of respondents identifying stage
---|---
Project Initiation and Planning | 7
Feasibility Study | 3
Systems Analysis | 18
Systems Design | 23
Coding/Programming | 4
Testing | 8
Implementation | 6
Training users | 3
Embed in the whole process | 11

Table 2: Stages in the systems development lifecycle that offer opportunities for PDP enhancements

Systems analysis and design are identified as being the areas in which the greatest contribution can be made. It is worthy of note that systems design is the most frequently stated stage whilst in the roles identified in Table I it does not feature prominently. This issue will be subject to further data analysis with regard to identifying which particular roles were identified by those including systems design as a stage that offers PDP opportunities. The lack of prominence for systems designers in Table I may be a matter of terminology rather than an accurate reflection of professional practice or perception.

The third most frequent response was an unprompted ‘embed in the whole process’. Clearly, respondents reporting this felt strongly that PDP awareness and practice should be present in all aspects of IS work. Whether this is a reflection of the managerial composition of the respondent group or a more general feeling amongst the profession will be subject to further examination and reported upon at a later date.

Evidence has been presented that shows that IS staff have an important role to play in the provision for PDP and this section shows which IS roles can contribute mostly and in what stages. We now go on to consider the final research question this paper reports on.

6. Are IS staff equipped to meet the challenge?

Identifying IS staff as instrumental in providing systems that facilitate PDP mean that it is crucial that this group are aware of both the framework and their responsibilities within it. We have seen how at a national level IS staff have been identified as critical to the implementation of PDP within organisations and within information systems. It has been reported here that IS staff accept that responsibility and can identify roles and opportunities for contributing to PDP. This section considers whether the profession is ready to meet these challenges and if not what needs to be done to better support IS staff in meeting the challenges they readily accept.

A starting point for this analysis concerns levels of awareness with regard to PDP and the legislative framework within which it sits. A simple question to address is, ‘how aware are IS staff of PDP issues?’. Levels of PDP awareness amongst the
respondent group were reported as high. Eighty eight percent reported that they knew how the principles found in the 1998 Data Protection Act affect the development of IS and their subsequent operation. It may be that this high level of awareness is a reflection of the composition of the respondent group rather than a broader reflection of awareness in the IS hinterland. Those that responded may simply be the IS staff that are actively involved in provision for PDP and as such they may be more knowledgeable than their colleagues. Further research is to be undertaken to explore levels of awareness amongst different IS staff groups and into what they actually mean by 'high'.

Looking at the IS profession as a whole, 36% felt that awareness of the 1998 Data Protection Act amongst IS staff is high, whereas 45% felt that it was not. Respondent characteristics and their individual responses to this particular question will be examined in an attempt to identify any correlations that may inform these findings. For example 60% of responses came from personnel in organisations that have more than 1000 employees. It may be that awareness in companies such as this are higher than the industry standard due to formal training opportunities that may exist more in larger organisations than smaller ones. It may also be that what is being reported here is a management view of levels of awareness rather than the view from a broader body of IS staff. Completing a questionnaire on data protection may appeal more to 'privacy advocates and or privacy professional’ than to other IS staff that may feel exposed by a lack of awareness or uncertainty with regard to PDP. Further research using case study approach will explore this in more detail.

These findings are supported by preliminary analysis of the 2002 IMIS Survey (Prior, Fairweather and Rogerson 2002) which shows that out of the 31 responses received at the time of writing 19% felt that awareness of data protection amongst IS staff is high whilst 68% felt that it is not. This survey reports less confidence in IS staff awareness of data protection. This may be because of differences in the respective respondent groups and will be examined further in subsequent research.

If IS staff are to design compliance into computer systems then they need to be operating in a context that is sensitive to and supportive of PDP. Clearly, designing a compliant system will be less effective if it is used in an organisation that does not provide a supportive environment and culture for PDP. It was found in the survey that 81% of respondents work in companies that have a general PDP policy for all staff. This appears a positive context for the development of systems that are compliant with PDP requirements. However, the following statement 'I have a detailed knowledge of my organisations policy for all employees' was responded to as follows:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disagree</td>
<td>24%</td>
</tr>
<tr>
<td>Indifferent</td>
<td>18%</td>
</tr>
<tr>
<td>Agree</td>
<td>26%</td>
</tr>
<tr>
<td>Strongly agree</td>
<td>32%</td>
</tr>
</tbody>
</table>

More than 50% feel that they have a detailed knowledge of their policies and again this may provide an opportunity to undertake respondent analysis to see whether any correlations emerge from the actual data to inform the figures given above. With
regard to the extent to which policies are understood by other staff in organisations. Levels of awareness are reported as being much lower. Forty-five percent report that their company policies are not understood by their colleagues, and 42% report that they feel that the same policies are not applied by their colleagues. If stated policies are not known or applied, this may undermine even the most robust computer systems. Data protection is as much about human systems as computer systems; PETs and effective systems design can assist in safeguarding against human failings but it cannot guarantee protection.

Based on the evidence presented, we conclude that levels of awareness for those that are active in the field of PDP is reported as being of an acceptable level but awareness amongst their IS colleagues is not of an adequate level. The survey sought information regarding training and support offered to IS staff. Not a single respondent agreed with the statement 'organisations are providing suitable training in PDP issues for employees.' Seventy-one percent disagreed with the statement whilst 29% were 'indifferent'. Ambivalence with regard to support being offered by professional bodies was also reported. 26% respondents felt that appropriate guidance was provided, 51% were indifferent whilst 23% felt that guidance was not provided.

In considering the question that prompted this discussion ‘are IS staff ready to meet PDP challenges?’ the data supports the following conclusions:

- IS staff are prepared to support PDP through their professional practice.
- IS staff have identified which staff can contribute and at what stage.
- IS and business managers have a fundamental role to fulfil in creating an environment in which PDP practices are understood and applied.
- Current levels of awareness of PDP issues amongst the general body of IS staff may be at a level that will not support them in meeting the objectives set by the IC of becoming a key player in developing privacy enabling systems. The reality of the ‘ethical engineer’ is perhaps not yet with us.
- Overall management strategy and commitment is as important as technical or procedural design factors.
- Training and further professional guidance is required at an industry wide level.

7. Further research

It was stated earlier in this paper that this report is concerned with one aspect of an on-going research project. Further research has already been identified to develop further the findings presented in this paper, these include:

- Increase the number of systems or business analysts, systems designers and programmers in the sample.
- Increase the number of small and or medium size organisations in the survey.
- Examine relationships that may exist in the data to inform the findings further. Many findings reported in this paper are tentative in that further data analysis may produce results that explain or highlight further relationships between variables.
• The role of systems designer is not as significant in the data as one may expect given the prominence they have in the literature. The reasons for this are to be explored further and reported upon at a later date.
• Explore the characteristics of the IMIS respondent group and the group that contributed to main body of data referred to in this report. This may provide insights in the reason for different levels of awareness being reported.
• Undertake a survey of IS education and training in PDP.
• Undertake case study research with a small number of organisations to explore with IS staff the contribution that they can make in the provision for PDP and how this impacts on IS practice.

8. Conclusion

It has been shown in this paper that IS staff are increasingly identified by government agencies and their representatives as critical to the successful implementation of privacy and data protection legislation. Evidence has been presented showing that this new role responsibility is accepted by members of the IS profession. Indeed, the evidence presented would suggest that IS staff positively support their involvement in safeguarding privacy and data. From this positive position it is possible to identify some factors that may need to be addresses in order for organisations to fully benefit from this support being offered by members of the IS profession. Paramount amongst these is the role of senior managers in creating organisational cultures and business practices that are fully supportive of PDP. Organisations cannot provide PDP through systems design, PETs and IS professional practice alone; the management context and wider organisational culture within which data is processed is, and always will be, critical to the provision of PDP.

References


Social and Ethical Impacts of Information and Communications Technologies (Rome: Libera Universita Internazionale degli Studi Sociali Guido Carli)


Introduction
This paper reports on research into the contribution that Information Systems (IS) staff can and do make to the provision of privacy and data protection (PDP) both technically, within information systems, and within organisations more generally. The research described in this paper forms part of an ongoing PhD programme of study and as such it gives an insight into one part of a much broader research process. The research described in this paper does however, represents a discrete and coherent topic that is worthy of consideration in isolation from the broader research.

This paper provides a background to the increasing need to recognise PDP as a major IS concern. It outlines the role of IS staff with regard to PDP as it is presented in the growing volume of literature. This is followed by a consideration of the research methods that have been used in those studies that contribute to defining the role of IS staff. This will lead to the suggestion of a ‘knowledge gap’ that is believed to exist and outlines further research that is being undertaken to address this gap. The methodology to be used in the proposed research is then outlined and justified. The research proposed in this paper is being undertaken during the period January – May 2004 and the preliminary findings will be presented at the ETHICOMP 2004 conference.

Background
The importance of PDP is now well established as a right for European citizens and this right is rapidly being extended to citizens of countries throughout the world. PDP has become acknowledged as a major concern of governments throughout the world leading to a ‘growing trend towards the enactment of comprehensive Privacy and Data Protection Acts around the world’ (EPIC 1999). The complexity and implications of global systems for PDP are increasingly acknowledged and in particular with regard to the USA and European trading relationship (Ross 2001). The importance of PDP is increasing to unprecedented levels and as a consequence understanding the developing role of IS staff is critical in supporting citizens in the information society.

The current role of IS staff with regard to PDP
Many researchers and commentators have contributed to discussion surrounding the role of IS staff in the development of privacy sensitive systems. These contributions are often expressed in an abstract or top-down manner, primarily concerned with
statements of principle rather than providing specific guidelines for professional practice. In the UK IS staff are increasingly identified by government agencies and their representatives as critical to the successful implementation of privacy and data protection legislation (France 2000, Rabb 1999). Elizabeth France in her role as the UK Information Commissioner (IC) actively promoted the concept of the 'ethical engineer', designing PDP into systems (France 2000). Anton and Earp (2000) promote the role of PDP in ecommerce applications and acknowledge that PDP is often an afterthought rather than a fundamental design principle. Lycett and Pouloudi (1999) considered ‘issues of data protection in contemporary development environments’ highlighting the ‘complex ethical debate for data controllers,.., the supervisory authority that oversees data protections, and information systems developers’. The IC, in her introduction to the Freedom of Information Act 2000, states that organisations will not be able to ‘determine their publications schemes if the presence and structure of data is not known’ (IC 2001). Clearly, IS staff are instrumental in structuring and providing access to an organisations data resources. Rabb (1999) has arrived at a similar conclusion to the IC and states that “those that design the systems and services with which they work are increasingly important as participants in the system” for PDP. He goes on to add that privacy-enabling technologies (PETs) are not just a technical fix that can be applied retrospectively, but should be applied as a fundamental part of the design process. Again the role of IS staff is critical in building into systems the provision for compliance with existing legislation and the flexibility to better meet the changing and unknown requirements of further legislation. Rabb (1999) goes on to report that the ‘UK Data Protection Registrar has discussed privacy issues with various large systems providers’ and ‘invited providers to design privacy into systems and for them to be part of the solution rather than the problem’. Prior (2002) shows how there is a strong belief amongst IS and business professionals that IS staff should ‘design data privacy and data protection compliance into information systems’.

This brief review of the literature regarding the role of IS staff in the provision for PDP shows quite clearly that systems design is seen by many as a key stage and process and it is not therefore surprising to see the UK Information Commissioner supporting further research in this area. The results of this research were published in draft form for consultation by Macaulay and Watts (2002). The consultation document, ‘Best Practice in Systems Design’, presents a set of systems design principles (known as ‘FARSTARS’: Fair, Adequate, Rights, Specific, Transfer, Accuracy, Retention & Security) and activities that if applied should increase the likelihood of privacy sensitive systems being developed. However, it should be noted that the guidelines are presented in seven pages and as such the work can only be realistically regarded as a starting point in this important area. There is a great deal more to be done both in terms of breadth and depth of coverage of these issues and the research reported upon in this paper seeks to contribute to this.

This review of the literature supports the conclusion that systems design is presented by many as a critical privacy enhancing activity within IS development. Whilst accepting the validity of this view the authors of this paper suggest that other systems development roles are as important, if not more important, than that of the designer. Moreover, it is suggested that accepting the design role as ‘the key activity’ may lead to less effective provision for PDP in organisations and systems in that other opportunities for PDP may not be recognised and or realised. Research presented at
ETHICOMP 2002 (Howley, et al 2002) provides insight into the provision for PDP within UK organisations that supports the view that other roles, activities and lifecycle stages are as important if not more important as systems design. Key findings were that:

- 95% reported that PDP is a legitimate activity for IS staff
- 81% felt PDP is an increasing concern for IS professionals
- in 26% of organisations IS staff have primary responsibility for PDP
- in 24% PDP is a shared responsibility between IS staff and DP officials.
- ‘IT/MIS/Systems Manager’ are the most important staff in bringing about PDP within systems
- The life-cycle stage within which opportunities exist for embedding PDP in systems were identified as being (in order of importance) Systems Design, Systems Analysis and ‘embed in the whole process’ of systems development.

This research offers support for the conclusions arrived at following the literature review; IS staff are important in the provision for PDP and that systems design is an important activity. However, we now have to add that other IS roles are also important and that these need to be as fully understood or explored as the systems design role. Before considering how these findings contribute to the research that is currently being undertaken it is necessary to consider the research methodology and respondent profiles of the research that gave rise to the conclusions.

**Methods and respondent profiles used in determining the role**
The initial evaluation of the FARSTARS concept (Keeling 2001) focuses on systems design and uses data that was gathered by means of:

- ‘depth and mini telephone interviews’,
- free text comments sent by post or email, and
- completion of a ‘basic evaluation form’.

This evaluation, which was undertaken by an independent researcher using data from 20 organisations and a population of Computing and Information Systems students, shows a positive and supportive response. Many respondents reported that they would adopt the FARSTARS principles in their systems practice. Following this positive feedback the originators of FARSTARS principles went on to revise the principles and publish the draft guide to systems design (Macaulay and Watts 2002).

The Howley Study (2002) was undertaken by the use of a questionnaire to which 42 usable responses were forthcoming. The respondent profile for this study is worthy of note at this stage as it provides additional insights into the conclusions drawn. The majority of respondents in the survey were ‘managers’ in ‘large organisations’. Most respondents had the word ‘manager’ in their job title and a large majority were from organisations with more than 500 employees. This respondent profile may have implications for the validity of the conclusions arrived at and this is considered in more detail in the next section.
The approaches to data collection used by Keeling (2001) and Howley (2002) can be classified as quantitative. The research methods used in both of these studies and their respective respondent profiles may justify the conclusion that they both lack detailed qualitative insights. Indeed, perhaps in recognition of this, the author of the FARSTARS Evaluation recommends that case study research be undertaken to monitor the implementation and development of FARSTARS (Keeling 2001). Howley (2002) concludes the 2002 study by suggesting that it is necessary to 'undertake case study research with a small number of organisations to explore with IS staff the contribution that they can make in the provision for PDP and how this impacts on IS practice'. Given this, the next section of this paper outlines a perceived knowledge gap which is followed by a proposal for research to address this gap.

The knowledge gap
The existing literature defines the role of IS staff as one primarily concerned with systems design. However, a review of respondent profiles and research methods shows that both the Howley Study (2002) and the Keeling (2001) evaluation of FARSTARS relied on quantitative approaches representing views from several industry sectors. Whilst no data is available from the FARSTARS study regarding the particular 'job titles' of respondents, this data is available for the Howley Study. The major respondent group in the study were managers from large organisations. This respondent profile may mean that the survey and its conclusions are representative of a partial view of the IS profession and its practices. The research proposed in this paper seeks to gain an insight into a more subjective view of PDP provision within IS practice and organisations. This research takes a broader view of IS staff roles and seeks to explore the PDP opportunities that may exist within all lifecycle activities and roles. The research seeks to gain subjective insights from all levels of IS staff rather than relying on a 'managerial view' gathered from quantitative methods. The data this research will be based on may be regarded as qualitatively richer than previous studies and as a consequence of this, the research may provide insights that were not identified in previous research in this field.

To summarise, the knowledge gap is concerned with the contribution to PDP that can be made in all IS development stages, by all IS staff and in different organisational settings. Previous studies in this field have focused on systems design (Macaulay and Watts 2002) as the key activity and the Howley Study (2002) is based on data that is, arguably, not representative of all levels of IS staff or organisational contexts. The research proposed in the next section seeks to address this gap.

Proposed Research
This ongoing research seeks to provide an insight into the 'missing view'. The survey showed a high degree of acceptance for PDP responsibilities amongst IS staff and a high level of PDP awareness amongst respondents; further work needs to be undertaken to assess the extent that this is truly reflective of IS staff. This research seeks deeper insights into the views of IS development staff than previous research achieved. In particular, the research will seek to gain the views of systems or business analysts, systems designers and developers. These are the groups that previous research identified as having the greatest contribution to make in providing for PDP, yet they were not prominent in the respondent profile. The research will also seek to increase the number of respondents from small and or medium size organisations in
the study in an attempt to test whether the findings of the survey are representative of large organisations only.

The study will build upon earlier survey results into levels of awareness and activities within which IS staff can make the best contribution. The proposed research will seek to address several related research questions, they are:

How aware are IS staff in the selected case study organisations of PDP legislation and developments?
Who actually is responsible for assuring PDP is considered in IS development and operation?
What do IS staff actually do to assure that their systems and practices are PDP sensitive?

Once answers to these questions are forthcoming certain key challenges will be identified that face both the IS professional and the organisations they represent. This will culminate is a proposed strategy for action.

**Theoretical issues**
The provision for PDP within organisations cannot be divorced from its context and as such the proposed research will provide an opportunity to explore the theoretical links between ‘context and outcome’, ‘motive and action’ and ‘structure and agency’. The research will provide an opportunity to assess the extent to which three theoretical strands inform our understanding of the provision for PDP. In particular the role of policy networks (Marsh and Rhodes 1992), Actor Network Theory (Callon 1991, Latour 1992) and Structuration (Giddens 1984) will be considered as theoretical frameworks for the interpretation of case study data. The extent to which these theoretical positions supports this research will be presented at the conference.

**Methods used to support the proposed research**
Interviews are the primary research method used in this research and these interviews will be undertaken within selected case study organisations. The case study approach can be adopted when detailed insights on issues are sought from either a single or small group of organisations. Case study research can be used to focus on a set of issues in organisations in an in-depth manner. Yin (2003) suggests that case study is a widely accepted research method that ‘investigates contemporary phenomena within its real-life context especially, when the boundaries between phenomena and context are not clearly evident’. This research is concerned with the relationship between the IS professional, the emerging PDP responsibility and the organisational context; the boundaries within this ill-defined space are not clearly evident and as such are suited to case study investigation.

There is a strong tradition (Walsham 1995, Klein and Myers 1999) of case study research in IS and this supports the selection of case study as an approach to use in this on-going research. Myers (1997) states that ‘case study research method is particularly well-suited to IS research, since the object of our discipline is the study of information systems in organisations’ Given this suitability it is no surprise that Myers goes on to suggest that case study research is the most common qualitative
method used in IS research. Klein and Myers (1999) argue that ‘case study research is now accepted as a valid research strategy within the IS research community’.

The interpretive approach to case study research is outlined by Walsham (1995). He suggests that interpretative case studies seek to contribute to our understanding of the context and processes that surround the use and development of information systems in organisations. Klein and Myers (1999) add that a case study is interpretative ‘if it is assumed that our knowledge of reality is gained only through social constructions such as language, consciousness, shared meaning, documents, tools and other artefacts’. This approach focuses on the meaning of social action as interpreted by the actors involved in the construction of that very same social action. In the interpretative case study the interpretation of events by the researcher cannot be done in isolation of the socially constructed and forever changing context, social relationships, formal and informal structures and processes.

A feature of the anthropological tradition that Walsham brings to interpretative IS case studies is the concept of ‘thick description’. In attempting to understand a complex reality that is reported though many ‘interpretations’ one has to seek the fullest and deepest (ie. ‘thickest’) understanding before any conclusions can be reliably reported. It is intended to seek a detailed and pluralistic understanding of a situation. Accepting one interpretation of any reality too readily, no matter how closely it meets our expectations or theory, can lead to serious misunderstandings on the part of the researcher. Walsham (1995) suggests that:

‘the ethnographer is faced with a multiplicity of complex conceptual structures, many of them superimposed upon or knotted into one another and which must be first grasped and then rendered intelligible to others. The IS researcher entering an organisation today is also faced with complex and intertwined conceptual structures which it is difficult to grasp and make intelligible....... The need for ‘thick’ descriptions is ..... important in trying to understand what is happening in connection with complex computer-based information systems, involving managers, users and designers’.

Organisational life and its artefacts are hugely complex and ever changing; seeking to realise reliable and robust ‘second-order’ data requires a thorough and detailed understanding of the motives and subtleties that mediate IS practice in organisations. Walsham (1995) adds that ‘an IS researcher can only access these subtleties of changing interpretation by the use of approaches based on ‘thick’ descriptions’.

Yin (2003) suggested that the case study method is best used when the research seeks to answer ‘how’ and ‘why’ questions. Walsham (1995) agrees that case study research within the interpretive framework can usefully address these types of questions. The research outlined in this paper is concerned with ‘How is PDP provided for in organisations and within systems development?’ and ‘Why is it done that way?’. Given that ‘how’ and ‘why’ questions feature so prominently in the proposed research it is suggested that the case study is an appropriate method for supporting this research.
This research will be characterised by discipline and rigour in design and interpretive in implementation and analysis. The work will seek to gain rich insights and ‘thick descriptions’ that allow for a subjective view of IS PDP practice to emerge.

Findings to be presented at the conference
As stated in the introduction to this paper this research is ongoing and as such the findings and analysis will be presented at the conference under the following headings:

- Case study profiles.
- Who does PDP, how and when?
- Who can do PDP, how and when?
- PDP: The IS professional challenge.
- PDP: The organisational challenge.
- PDP: A strategy for action.
- The theoretical perspective.

Conclusion
The research reported on in this paper builds on earlier research reported to ETHICOMP 2002 and as such it represents a ‘next stage’ in further understanding the role of IS staff in providing for PDP. The case study research currently being undertaken will provide detailed subjective insights into the provision for PDP within organisations. These insights will complement and advance our understanding of this important and complex field and enable the IS profession to better support citizens in the information society.


Howley, R., Rogerson, S. and Fairweather, N.B.
‘The Data Protection Decade 1995-2005’

Abstract

The ETHICOMP decade is also the ‘data protection decade’. On 24th October 1995 the European Commission adopted Directive 95/45/EC on ‘protection of individuals with regard to the processing of personal data and the free movement of such data’ thereby creating the foundation for current European Data Protection. A decade later it is an appropriate time to review how organisations and their Information Systems staff have responded to the challenges of a data protection decade. This paper presents the findings of case study research into how the management and development of information systems have responded to data protection challenges. Whilst the emerging findings show a commitment to the protection of data by information systems staff and their management there is little evidence that data protection has become a formal and valued part of the information systems development process. The authors consider these findings in the context of a changing world and one in which the uses to which data is put are constantly challenged.

Introduction

The ETHICOMP decade is also the ‘data protection decade’. On 24th October 1995 the European Commission adopted Directive 95/45/EC on ‘protection of individuals with regard to the processing of personal data and the free movement of such data’. This Directive created the foundation for current European Data Protection legislation and much of the legislation that followed worldwide (EPIC 1999, Lederman, Shanks and Gibbs 2003). Thus commenced the data protection decade.

The volume of data and the uses to which it is put have grown rapidly to exploit business opportunities in the Internet age. Data is global, highly mobile, shared, abused and as well as being an increasingly important business asset it has become a key element of national defence in a war on terror. Each development presents huge challenges to those seeking to use and protect data and those seeking to establish and maintain national and trans-national schemes for protection of data.

The decade has also seen increasing recognition that information systems and information systems staff are key players in data protection provision. A major focus of related UK research has been on the importance of the systems design stage of the development process, resulting in a set of ‘Best Practice Guidelines in Systems Design’ (Macaulay and Watts 2002). Other research (Howley et al 2002) sought insights into levels of data protection (DP) awareness amongst information systems (IS) staff and how they can and do contribute to DP. Whilst IS staff support DP, awareness of its issues was relatively low. Thus their contribution to the ‘data protection decade’ may be less than it could otherwise be.
Case study research has been implemented during 2004/5 into how three UK organisations are responding to DP and its challenges. Firstly, however it is appropriate to provide insights into the research and data analysis design as well as some background to the case study organisations.

Research Design
This research builds on previous quantitative research (Howley et al 2002), seeking to provide detailed insights into how a small number of organisations are responding to increasing DP demands. Case study research was identified as most suitable in seeking these insights. Case studies are widely regarded as an appropriate method within IS research (Walsham 1995, Klein and Myers 1999). Myers (1997) states that ‘case study research method is particularly well-suited to IS research, since the object of our discipline is the study of information systems in organisations’. This research seeks insights into two questions about IS staff in organisations:

1. What professional responsibilities are IS development staff seen as having in providing for DP?
2. What role is attributed to IS management in providing a context and framework for DP?

These two questions focus on IS practice in organisations, hence the choice of case study research is fully supported. According to Yin’s (2003) classification this research is a descriptive and explanatory case study. Research will provide descriptions of, and explanations for, patterns of response to DP requirements found, and their relationship to context. The research focuses on three case study organisations, with two units of analysis in each case. One industry sector is chosen, Local Authorities in the Midland region of the UK.

A range of theoretical propositions emerged both from earlier qualitative research and with the design and implementation of case study research. Theoretical propositions that guide the research, and the conceptual model that contextualises it, are fully represented in the case study protocol. Theoretical propositions that guided the case study design and implementation include:

1. There is a commitment amongst IS staff to support data protection.
2. Organisations face similar challenges in responding to DP regardless of their size and complexity.
3. Levels of awareness may be too low to effectively respond to DP challenges.
4. Levels of commitment amongst IS staff may vary in a consistent manner at different levels of an organisation.
5. Little is being done to embed DP practices in the systems development process.

It is now appropriate to briefly profile the case study organisations.

Case Study Organisations
Three local authorities from the central regions of England contributed to this research.

1. A rural Authority in a relatively small market town serving a population of approximately 75,000 and covering approximately 230 square miles. Seven permanent staff and a separate E-Government team support the IT function. The IT
function draws upon consultants for specialist and extra support at times of particular need. The IS Manager/DP Officer and a Senior Developer contributed to this research.

2. A County Council serving a large population located in a mixture of county towns and villages. The authority has a knowledgeable, dedicated and active DP Officer and a ‘centrally managed-locally delivered’ IT function. The Applications Development Manager (ADM) has approximately 63 full-time equivalent staff. They are in four major service departments with the IT function within each being managed by a Departmental IT Manager. The ADM and IT Departmental Managers control development staff, project managers, systems analysts and business consultants. The ADM and four Development Team Leaders contributed to this research.

3. A unitary Authority serving a large town and its surrounding district which in itself contains a further six small to medium towns. DP within this authority is managed through the work of a DP Officer who is a member of the IT team. The IT function is supported by four full-time retained staff, the IT Manager, the DP Officer, a Freedom of Information Project Worker and an E-Government Project worker. Apart from these roles the IT function has been outsourced to an IT services provider as part of a Public-Private Partnership. Many of IT staff that worked for the authority now work for this IT services provider. The IT Manager, the DP Officer and three development staff contributed to this research.

Data Analysis Design
Data analysis is an issue that was considered early in the research process and a range of data analysis issues are presented in the case study protocol. The strategy draws on recommendations made by Yin (2003), Marshall and Rossman (1999) and Mason (2002). Data analysis involved: Organising, structuring and indexing data. Data was organised in a number of ways to facilitate analysis, including by theme, research question, organisation and occupational role. The research questions and theoretical propositions suggested codes or patterns that were likely to be prominent in data analysis. Codes included: ‘awareness’, ‘training’, ‘development stages’, ‘commitment’, ‘legitimacy’, ‘staff’, ‘effectiveness’ and ‘policies’. These were the preliminary set of codes and as expected with qualitative research these codes were refined and added to during research and data analysis. Data is being analysed using NVIVO (QSR International Software 2003) qualitative data analysis software. As new codes or emergent themes are identified data is being re-examined to assess contributions to interpretation. Emerging and sometimes rival interpretations are being identified and reviewed with regard to their contribution to the research.

We can now consider some findings that are emerging.

1. How data protection is provided for and managed within these organisations and an evaluation of the effectiveness of these processes.
All three organisations have a nominated person responsible for DP. Organisations two and three have a nominated person performing a dedicated DP role. In organisation one DP responsibility was administered by the Information Services Manager. Organisations two and three have formalised structural arrangements for DP. In organisation two there are two parallel strands working together. The DP Officer describes DP provision as “a decentralised approach with extensive provision for induction, training and information dissemination”. The DP strand is managed by the Compliance Officer who works with nominated DP Liaison Officers within each service department. The IT function/strand is also decentralised with the ADM at the core and a
team of managers working with their IT teams in each major service department. There exists multiple communication channels active within this network providing both horizontal and vertical support to DP provision. DP within organisation three is similar in that the DP Officer works with a team of departmental representatives who deal with DP locally. DP within organisation one is less structurally defined but is perceived to work well and be supportive of their needs. All organisations have a range of DP policies in place and evidence of extensive training provision was forthcoming.

The DP Officer at organisation two is relatively new to post and inherited the structures outlined. He acknowledges that liaison through the DP hierarchy does not work perfectly and he will be addressing this issue. In organisations two and three a potential tension was reported about the operation of the DP management strategy relying on departmental staff involvement when their commitment may be limited due to their other departmental commitments being given priority. The smallest organisation reported relatively simple yet effective DP management processes which were highly personalised and supported by documents and training. The third participating organisation outsources its IT services and the DP Officer has a DP liaison role both internally and externally. This participant pointed out that the DP Officer needs a high organisational profile to effectively deliver DP, he said that ‘positioning the data protection person is critical to securing compliance’.

When asking participants to evaluate their own DP provision and its management a range of responses were forthcoming. Statements such as ‘reasonable’, ‘not confident with DP” and ‘medium’ came from middle managers and developers whereas senior colleagues were inclined to use phrases such as: ‘good, its engrained in the work we do’, or ‘its quite good’. Structurally and procedurally DP is well provided for, but there are issues which may undermine DP provision and its management. In one organisation there was a frequently reported belief that DP compliance is less important than meeting targets for delivering systems. Comments such as, “the priority is to make things work, not DP” and “if you are not implementing because it doesn’t meet one of the tenets of the DP Act, it would just carry on past you. It’s about being able to deliver things … primarily” support the view that real commitment to DP by some IS staff has some way to go. Tension between delivery schedules and DP compliance may represent an unequal relationship between two professional responsibilities.

2. IS staff and provision for DP

This section reports on relationships between IS staff and organisational structures for DP and specific contributions that IS staff can and do make to DP provision.

There is a strong link between DP procedures and IS staff within all cases. DP responsibility is either currently located within the IT Department or it had been until relatively recently. This would suggest that a close and mutually supportive relationship can exist between the two services. In all cases it was stated that DP is most effectively delivered through a partnership involving user departments and IS staff. In all three organisations there is a consistent belief that the data belongs to user departments and as such what they do with data, including legal compliance or otherwise, is their responsibility. Whilst the users of IS in all organisation can and do use their DP and IS staff as a source of information and guidance regarding DP, IS staff feel that primary responsibility for DP lies with users. The following comments illustrate the depth of this view: ‘development staff only see their responsibility to DP in a general way – it’s the user department’s data and it’s their responsibility’. A Development Team Leader commented that whilst DP is part of his job it has to be done in partnership with users.
Overall relationships between DP Officer, IT Managers, developers and end users were not clear with regard to DP issues and in particular their contribution to IS development. DP Officers were not structurally supporting systems development and systems developers were not uniformly active in supporting DP; role ambiguity with regard to DP was the norm.

In examining the specific contribution that IS makes to DP provision this research develops research regarding the role of IS staff, reported at ETHICOMP 2002 (Howley et al 2002) and that undertaken in Australia (Lederman, Shanks and Gibbs 2003). That research found emphasis on systems design and data quality as key to effective DP provision and suggested that other activities may offer the same or more opportunities for DP leverage; this discussion seeks to address this uncertainty.

Participants were asked questions concerning:
1. What stages/activities offer the greatest potential for increasing Privacy and Data Protection?
2. Which IS staff do you think can contribute most?
3. Which data protection principle(s) can IS staff make the greatest contribution to?

The most frequently identified stages were: business analysis, project initiation, feasibility study, ‘up-front activities’, ‘build in security from day one’, design, training, programming and testing. Throughout, emphasis was on early life-cycle activities with no noticeable variation between occupational role and response. It is notable that life-cycle coverage is provided but was not necessarily articulated by respondents.

The most frequently identified staff, not surprisingly, correspond to the stages identified and include: Business Analysts, Developers, Project Managers, Designers and Systems Analysts. It was frequently stated that those that set-up projects have particular responsibility for establishing DP issues and assuring their prominence in what follows. This view was expressed by respondents at organisations two and three. A recurring problem faced by development staff was reported by a Development Team Leader in organisation two when he stated that ‘development staff have no DP reference points to assist [them] in compliant design. Levels of awareness are very much background’.

With regard to UK data protection principles there was a strong focus on Principle 7 (the application of appropriate technical means to secure data). This was not surprising, but the overwhelming enthusiasm for participants to recast their DP responsibilities in ‘Security’ terms was. Many respondents sought to talk about security claiming that it is synonymous with data protection. A Development Team Leader in organisation two explained ‘when I say security what I’m talking about is privacy and data protection ... I think the two things go hand in hand’. The Senior Developer in organisation one responded to the question ‘Is DP a legitimate concern of yours?’ with the answer is ‘I think it’s relevant because the more you can concentrate on these things at source the better. There is no good trying to apply security to the system after it’s been developed. If we control security of data it means the DP task is a lot easier’. This comment supports the view that supporting DP in systems development should come early in the life cycle and secondly shows the single-minded focus of this developer on security. The question was about ‘legitimacy’ not ‘security’.

When prompted most respondents could and did give examples of how their work can and does support all the principles and this confirms earlier research (Howley et al 2002) which claimed that IS staff have a role encompassing the whole life cycle and supporting all DP principles.
However, unprompted responses to the question, ‘Which principles can IS staff best support?’ usually led to the immediate identification of Principle 7 followed by principles concerned with volume of data, use to which data is put, retention periods and data quality, i.e. accuracy and integrity. The overwhelming view of many respondents is that DP is synonymous with security, whilst the view of the authors, and some DP Officers in this study, is that it is much broader than that.

The emphasis on security is interesting on a number of fronts. Firstly, it can be seen as an entirely reasonable and appropriate response to increasing privacy and DP requirements. Data professionals have always been the guardians of data and as such internalising or interpreting DP requirements in terms of ‘security’ provides a familiar context within which IS staff can formulate their response to DP requirements. In this respect this is an effective and positive response to DP legislation and increasing privacy awareness. However, a slightly less desirable consequence of this emphasis may be that it allows those involved to avoid formulating an IS response to other requirements in the DP principles. Almost all respondents had to be prompted to consider principles beyond principle 7 when considering their contribution to DP in systems development. This emphasis on security may artificially limit their contribution. Once prompted and provided with examples of how IS staff can contribute more widely, respondents were enthusiastic about these suggestions. Discussions at this time led to the identification of a number of ways that IS staff can contribute more effectively and these are considered in the next section.

The research sought the views of IS staff with regard to the extent DP is legitimately their responsibility. Frequently it was reported that DP is a legitimate concern of the IS professional because ‘we are data professionals and as such we care for data’. Another respondent reported that ‘we deal with data responsibly, because we are responsible people’. As with the security issue, this may be an example of IS staff responding to new challenges by locating them within their existing framework of professional expectations rather than seeking to develop, and therefore accept, a broadening of their role. At management level there is a total acceptance of DP as a legitimate concern of IS staff but amongst developers different opinions surfaced. A statement made by a developer, as the discussion became more relaxed and open, that DP was a ‘pain in the neck’ was roundly supported and enjoyed by his colleague. When asked ‘if data security is a pain in the neck’ he responded immediately, ‘No. It’s a pain in the neck if we don’t deal with it’. ‘Data Protection’, for this respondent was not highly valued, but ‘Protecting Data’ is. This may provide a fundamental insight into the perceived value of externally imposed responsibilities on the IS role, i.e. the need to accommodate data protection, compared with the higher value that may be placed on an internal and professionally developed response to a new responsibility or a broadening of the IS role, i.e. increasing the protection of data.

This discussion also gave rise to an insight that is worth reporting now. The emphasis on security amongst IS staff may be at variance to views expressed by one DP Officer. The Compliance Officer at organisation two suggested that interpreting DP at an organisational and professional level as a security issue is a response typical of IS professionals. He suggests that by doing so they may be missing important opportunities to improve the service they provide data subjects. He stated that the Act is about ‘accessibility not inaccessibility ... a large cultural shift is needed [to change the mindset of IS staff] and this will take a long time to occur’. His view was that IS staff traditionally have viewed data as something to be ‘locked-down’ and controlled tightly. On the other hand he regards the most effective response to the increasing need for formal DP provision is to unlock data and make accessibility and openness the basic design and operational principles. This view was supported by the developer in organisation one who stated that they wanted to ‘give users as much flexibility as possible - let them use their common sense’ when
creating their own systems and accessing corporate data. A developer at organisation three adds ‘before you get to the point of creating any software you have to know what you are protecting it against, who you are protecting against and who needs access’. The DP Officer believes that this represents a fundamental shift in thinking from that presented by many IS staff. This may provide an important area for future research or an emerging theme of this research.

3. Specific insights were sought into how information systems development practices support the creation of systems that are supportive of data protection.

Previous research (Howley et al 2002) and professional guidelines (Macaulay and Watts 2002) highlight the importance of systems design and suggest that project management is of equal importance. This case study research sought the views of all respondents into how ‘DP could be better provided for’ and a range of responses were forthcoming. Interestingly, this part of the interview/discussion process not only provides answers to the question ‘how can we do it better’ but it also serves to triangulate the responses to earlier questions. Specific suggestions made by respondents for dealing with DP better included:

1. Increase awareness. This was reported by many respondents and covers not just ‘what is the Act’ and ‘subject access’ but was extended to include ‘how to develop DP compliant systems’. DP training is provided in all organisations but no training was reported in the area of IS development and DP.

2. Including the DP Officer at key points of the systems development cycle, i.e. part of the project team. This suggestion emerged out of more than one discussion and was seen as representing a positive opportunity to embed DP within systems development as well as formalising the relationship between DP Officers and their IS staff. In organisations where systems are developed by the users in departments it was felt that the responsibility for DP compliance should be more clearly defined. Developers in all organisations feel that it should be the user’s responsibility, but accept that ambiguity exists still with regard to current DP responsibility.

3. The relationship and relative responsibilities of the DP Officer, IT Managers and Developers could be more clearly defined in an operational way.

4. Provide a set of principles or guidelines of what DP consideration can and should be applied at each stage of a development process. The desire to avoid checklists that simply get ‘ticked’ but otherwise ignored was reported more than once but some developers were open and enthusiastic about the need for clear guidance with regard to how and when they can support DP.

The Research Questions and Theoretical Propositions

This research was designed to address two related research questions and their supporting theoretical propositions. It is appropriate to review those questions and propositions in the light of the findings presented.

<table>
<thead>
<tr>
<th>Question/Proposition</th>
<th>Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>What professional responsibilities are IS development staff seen as having in providing for DP?</td>
<td>Development staff and their managers in this study readily accept responsibilities in the complex arena in which DP is provided for. They see their role primarily in terms of applying security to their user’s data. The emphasis is very much on ‘the users’ data and ‘the users’ system.</td>
</tr>
<tr>
<td>What role is attributed to IS management in providing a context and framework for</td>
<td>Management are clear regarding their role in DP provision; it is advisory, consultative and assures data integrity and security. It is primarily one of close liaison horizontally with other IS and or DP managers and vertically through IS structures and staff.</td>
</tr>
</tbody>
</table>

257
There is a commitment amongst IS staff to support data protection. This finding from earlier research (Howley et al. 2002) has now been confirmed both in this research and by other surveys (Prior et al. 2003 & forthcoming).

Organisations face similar challenges in responding to DP regardless of size and complexity. Even though the three organisations that contributed to this research varied considerably in size, organisation and responsibilities, they consistently reported similar concerns and interpretation of challenges that face them and how to respond to those challenges.

Levels of awareness may be less than required to effectively respond to DP challenges. ‘Levels of awareness’ was frequently reported as an issue for those involved in this study. Obviously, care has to be taken drawing conclusions based on such deeply qualitative expression, however, in the area of DP and specifically systems development strategies for compliance it is felt that awareness could be increased. All these organisations have effective and comprehensive provision for general DP induction and training, but in the field of IS development there is much still to be done before the era of the ‘ethical engineer’ is with us.

Levels of commitment amongst IS staff may vary in a consistent manner at different levels. Whilst there is some evidence in the data that the more senior you are, the more likely you are to accept DP as a legitimate concern of IS staff, interpretation of this data is ongoing. Willingness to accept a responsibility for DP by senior IS staff may have more to with the history of DP in their organisation and or political expediency than actual commitment. Clearly, both of these responses, if supported by the remaining evidence, are wholly reasonable.

Little is being done to embed DP practices in systems development process. This proposition is fully supported by the data. Security is recognised and well provided for, but it was agreed that much more can be done across all stages and supporting all principles. This will become a future research activity for the authors of this paper.

This research has addressed a range of research questions in the area of DP and IS development. The findings presented in this paper triangulate in a supportive way earlier research findings that resulted from quantitative research (Howley et al. 2002). The outcomes of this research add confidence to both sets of findings and highlight important areas of future research and professional support that can still be undertaken and provided.

A great deal has been achieved in the Data Protection Decade; national schemes for DP now exist in most nations throughout the world and many are based on the European Directive that marked the start of the decade. However, DP provision may still have to face its biggest challenges - balancing needs for privacy and data protection with a need to maintain physical security in an increasingly dangerous world. How this battle is fought and who ‘wins’ may turn out to be one of the defining features of the ETHICOMP decade.
Defining features of the ‘ETHICOMP/data protection decade’

In the first half of the decade huge strides forward were made globally in identifying data subjects’ rights to privacy and data protection. These were enacted throughout Europe half way through the decade and similar, but locally sensitive systems for protection of data, were put into place throughout the trading world thereby allowing for ongoing trading relationships and in recognition of rights to privacy and DP. In the second half of the ETHICOMP decade conflict between ‘rights’ for privacy/DP and needs for physical and national security has arisen. Global terrorism is seen as a threat to citizens and this is leading to changes in data laws and in perceptions about those laws. Some powerful nations may be unilaterally dismissing national schemes for data protection if those schemes appear, to the powerful, to be counter to their perceived needs of national security. Global responses to this challenge may well provide a real insight into our real commitment to DP and thereby define the DP decade for us.

Conclusion

This paper has presented tentative findings of case study research that has been undertaken into the role of IS staff in the provision for DP. Findings support earlier research in this field and identify new avenues for investigation. IS staff are committed to supporting the protection of data in organisations; and from a security point of view, those that contributed to this study do this very well. Significant opportunities still remain for DP leverage in systems development, through the embedding of DP sensitive development techniques, stages and or considerations. This is an area that the authors will continue to investigate and report upon.

Reference:


SAGE Publications


Increasing attention is being given to the contribution that information systems (IS) staff can make to the implementation of the 1998 Data Protection Act and the 2001 Freedom of Information Act in the UK. A focus of this attention has been on the contributions that can be made in the systems design process and in the application of privacy enabling technologies (PETs).

Recent research by the Centre for Computing and Social Responsibility (CCSR) found considerable evidence that IS staff are promoted as key providers of privacy and data protection (PDP) both within organisations and within information systems areas. Literature from Europe, the USA and the UK highlights the importance of designing systems for PDP compliance, encouraging the application of PETs and relating data management strategies to the provision for PDP. Whilst witnessing the emergence of PDP legislation CCSR wanted to know the extent to which this responsibility, that was increasingly being articulated, was known about and accepted by IS staff in UK based organisations. If IS staff are becoming increasingly responsible for PDP in organisations the extent to which they are aware of their perceived contribution and the degree to which they support it will be critical to its realisation. The research addresses these issues by focusing on three key questions.

1. Are IS staff aware that the responsibility for PDP is increasingly being devolved to them and is it perceived by them as legitimate extension to their role?
Ninety five percent of respondents regard involvement in PDP as a legitimate activity for IS staff and 85% believe that it is an increasingly important part of their work. The acceptance of PDP as a legitimate part of their work is further evidenced by the nature of the involvement reported. Staff report considerable involvement in the area of PDP management and strategy. In more than 54% of organisations represented in the sample IS staff were 'prominent in formulating and implementing PDP polices'. In 30% of organisations IS staff are 'primarily responsible for PDP within [their] organisations'. This involvement evidences a considerable acceptance by IS professionals of their role in the provision for PDP. It also suggests that their involvement is much wider than that proposed in the literature.

2. Which IS roles do IS staff consider to have the greatest contribution to make to the provision for PDP?

Systems design and the application of PETs are widely reported in the literature as areas in which IS staff can contribute to PDP provision. The views of IS staff were sought with regard to which staff roles offer the greatest opportunity to contribute to the provision for PDP. The roles and number of times they were identified are given in the Table 1.

Table 1. IS roles in the provision for PDP

<table>
<thead>
<tr>
<th>IS Role</th>
<th>Number of respondents identifying role</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT/MIS/Systems Manager</td>
<td>23</td>
</tr>
<tr>
<td>Systems Analyst</td>
<td>15</td>
</tr>
<tr>
<td>Systems Developers</td>
<td>9</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>9</td>
</tr>
<tr>
<td>Network Manager</td>
<td>6</td>
</tr>
<tr>
<td>Systems Administrators</td>
<td>6</td>
</tr>
<tr>
<td>Project Manager</td>
<td>7</td>
</tr>
<tr>
<td>Programmers</td>
<td>3</td>
</tr>
<tr>
<td>IT Security Personnel</td>
<td>5</td>
</tr>
<tr>
<td>Support and Training</td>
<td>2</td>
</tr>
</tbody>
</table>

The single most important finding was the extent to which staff identified the role of management as critical in the provision for PDP. Indeed, some respondents felt so strongly about this, they annotated their response to add greater emphasis to their answers. The role of the systems analyst (including requirements analysis) is also prominent in findings and it is interesting to relate this to the prominence of 'systems design' as opposed to 'systems analysis' in the literature. We should not be seduced into thinking that we can
'design for compliance' if we are failing to manage the capture and realisation of requirements that are in themselves PDP compliant.

3. What stages in a systems development process do IS staff feel offer the greatest potential for embedding PDP compliance in information systems?

In the introduction it was reported that systems design and the application of PETs are frequently identified in the literature as key areas in which IS staff can contribute to PDP within organisations and their systems. The views of IS staff were sought with regard to the stages of the systems development process that they feel offer the greatest opportunities for PDP leverage. Table 2 presents the findings.

Table 2. Stages in the systems development lifecycle that offer opportunities for PDP enhancements

<table>
<thead>
<tr>
<th>Stage</th>
<th>Number of respondents identify stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Initiation and Planning</td>
<td>7</td>
</tr>
<tr>
<td>Feasibility Study</td>
<td>3</td>
</tr>
<tr>
<td>Systems Analysis</td>
<td>18</td>
</tr>
<tr>
<td>Systems Design</td>
<td>23</td>
</tr>
<tr>
<td>Coding/Programming</td>
<td>4</td>
</tr>
<tr>
<td>Testing</td>
<td>8</td>
</tr>
<tr>
<td>Implementation</td>
<td>6</td>
</tr>
<tr>
<td>Training users</td>
<td>3</td>
</tr>
<tr>
<td>Embed in the whole process</td>
<td>11</td>
</tr>
</tbody>
</table>

The role of management, which was identified so frequently in response to the previous question, may support the further identification of 'project planning' and 'embed in the whole process' in the responses to this question. Systems (and or requirements) analysis is prominent in these findings offering further support for the roles identified earlier. This is interesting in that this is a stage that may be presumed to occur before design, even in 'rapid' and or 'iterative' development environments, and as such the prominence of design in the compliance strategy may be inadequate without an equal emphasis on the analysis process. Whilst design is important, IS staff feel that systems/requirements analysis and project management are equally important, and they should not therefore be neglected by a focus on systems design in isolation of requirements analysis and overall project management.

Conclusion. There is considerable support by IS staff for their involvement in the provision for PDP. Indeed, they already occupy important strategic PDP positions in many organisations. IS staff are able to identify the stages in a systems development
process which offer potential for PDP enhancements and the staff that have the
greatest contribution to make. However there is evidence that certain issues need to be
addressed if we are to benefit fully from the contribution of IS staff. Levels of PDP
awareness amongst IS staff is felt to be low; more than 50% of respondents felt that IS
staff awareness of the 1998 Data Protection Act is not high. IS staff feel that the level
of training in PDP issues offered by organisations was low; only 3% of respondents
felt that organisations are providing suitable training in PDP issues for their
employees. Regarding support offered by professional bodies only 29% of
respondents felt that they provide appropriate guidance for members. Could such
bodies do more?

There is a management challenge that extends beyond the role of IS staff;
management have a responsibility to create and maintain a PDP culture within
organisations that positively impacts on all stages of IS development, the operation of
information systems and all staff. IS staff alone cannot bring about PDP compliance
through some form of technical wizardry, and nor can management. The provision for
PDP in organisations and within information systems has to be the result of a holistic
cultural and structural commitment to PDP that is bought about and maintained by
senior management within organisations. No one group of staff can affect PDP alone -
it has to be an organisational wide commitment and be embodied in the very core of
the organisation; this is the management challenge that must be addressed.

Please send your views on ethical and social responsibility issues and cases of ethical
dilemmas to:

Professor Simon Rogerson
Director
Centre for Computing and Social Responsibility
Faculty of Computing Sciences and Engineering
De Montfort University
The Gateway
Leicester
LE1 9BH
Tel:(+44) 116 257 7475
Fax:(+44) 116 207 8159
Email:<sro@dmu.ac.uk>
Home Page:http://www.ccsr.cse.dmu.ac.uk