Demonstrate and Document: The Development of a Best Practice Model for Biometric Access Control Management

Lynne Norris-Jones LL.B (Hons) M.A. FHEA

Thesis submitted to the Department of Information Systems and International Studies, Cardiff School of Management in partial fulfilment of the requirements for the degree of: DOCTOR OF PHILOSOPHY

(Director of Studies: Dr. Giles Oatley. Supervisor: Mr. Pat Cleary)

July 2011
DECLARATION

This work has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree.

Signed ......................................................... (Candidate)
Date ..............................................................

STATEMENT

This thesis is the result of my own investigations, except where otherwise stated. Other sources are acknowledged by explicit references.

Signed ......................................................... (Candidate)
Date ..............................................................

STATEMENT

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and abstract to be made available to outside organisations.

Signed ......................................................... (Candidate)
Date ..............................................................
Abstract

This thesis investigates the social, legal and ethical perceptions of participants towards the implementation of biometric access control systems within a sample of United Kingdom work-based environments. It focuses on the application of fingerprint scanning and facial recognition systems, whilst alluding to the development of more advanced (bleeding edge) technologies in the future. The conceptual framework is based on a tripartite model in which Maslow’s Hierarchy of Needs is applied to the workforce whilst the principles of Utilitarianism and the Psychological Contract are applied to both management strategies and workforce perceptions. A qualitative paradigm is used in which semi-structured interviews are conducted with management and workforce participants within a sample of United Kingdom-based organisations (represented by Case Studies A-D). Discourse from these interviews are analysed, leading to the development of a series of first-cut findings for suggested “Best Practice” in the social, legal and ethical management of biometric access control systems. This process is subsequently developed with a refined sample of respondents (Case Studies A and C) culminating in the presentation of a suggested “Best Practice Model” for application to all four case studies. The model is based upon elements of a pre-determined Code of Practice (ISO/IEC 27002 Information Technology – Security techniques – Code of Practice for Information Security Management) towards fostering acceptance of biometric technology within the workplace, in answering the question:

*How should organisations using biometric access control systems address social, legal and ethical concerns in the management of specific working environments in the United Kingdom?*

Acknowledgements

I would like to express my gratitude to the following people, without whom the completion of this thesis would not have been possible:

Professor Eleri Jones (my Mentor) Mr. Pat Cleary (Supervisor) and Dr. Giles Oatley (Director of Studies): for their advice and assistance throughout the process of this investigation.

The research participants: Dr. Fred Preston (for his advice and assistance during the pilot study) and those organisations who participated in the case study investigations at both management and workforce levels.

My immediate family (Keith, Owain, Gareth, Michelle and Rhys): for their support and tolerance.

My late father and grandmother: I miss you both.

Jack (my beautiful Boxer dog): who I haven’t walked regularly in a long time.
## Contents

<table>
<thead>
<tr>
<th>Chapter 1: Introduction to the Investigation</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Introduction</td>
<td>2</td>
</tr>
<tr>
<td>1.2 Background</td>
<td>3</td>
</tr>
<tr>
<td>1.3 Scoping the Research</td>
<td>3</td>
</tr>
<tr>
<td>1.4 The Research Problem and Question</td>
<td>5</td>
</tr>
<tr>
<td>1.5 Justification for the Thesis</td>
<td>5</td>
</tr>
<tr>
<td>1.6 The Research Agenda</td>
<td>6</td>
</tr>
<tr>
<td>1.7 Aim and Key Objectives</td>
<td>8</td>
</tr>
<tr>
<td>1.7.1 Aim</td>
<td>8</td>
</tr>
<tr>
<td>1.7.2 Key Objectives</td>
<td>8</td>
</tr>
<tr>
<td>1.8 Research Methods</td>
<td>9</td>
</tr>
<tr>
<td>1.9 Chapter Summary and Conclusion</td>
<td>10</td>
</tr>
<tr>
<td>1.10 Summary of Subsequent Chapters</td>
<td>10</td>
</tr>
<tr>
<td>1.10.1 Chapter Two</td>
<td>10</td>
</tr>
<tr>
<td>1.10.2 Chapter Three</td>
<td>11</td>
</tr>
<tr>
<td>1.10.3 Chapter Four</td>
<td>11</td>
</tr>
<tr>
<td>1.10.4 Chapter Five</td>
<td>12</td>
</tr>
<tr>
<td>1.10.5 Chapter Six</td>
<td>12</td>
</tr>
<tr>
<td>1.10.6 Chapter Seven</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 2: Literature Review</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Introduction</td>
<td>15</td>
</tr>
<tr>
<td>2.2 DNA Sampling, Biometric Technology and the Perceived Threat to Civil Liberties</td>
<td>15</td>
</tr>
<tr>
<td>2.3 Perceived Benefits of Biometric Technologies</td>
<td>18</td>
</tr>
<tr>
<td>2.4 Fingerprint Recognition</td>
<td>19</td>
</tr>
<tr>
<td>2.5 Facial Recognition</td>
<td>20</td>
</tr>
<tr>
<td>2.6 Universal Approaches to Fingerprint and Facial Recognition Systems</td>
<td>24</td>
</tr>
<tr>
<td>2.7 Biometric Access Control for Workplace Management</td>
<td>27</td>
</tr>
<tr>
<td>2.8 Initial Legal and Ethical Perceptions</td>
<td>35</td>
</tr>
<tr>
<td>2.9 Recognising Human Rights for Compliance</td>
<td>38</td>
</tr>
<tr>
<td>2.10 Privacy and Biometric Applications</td>
<td>39</td>
</tr>
<tr>
<td>2.11 Application of Privacy in Multi-Modal Systems</td>
<td>40</td>
</tr>
<tr>
<td>2.12 Application of Standards and Academic Projects</td>
<td>41</td>
</tr>
<tr>
<td>2.12.2 The British Security Industry Association (BSI)</td>
<td>48</td>
</tr>
<tr>
<td>2.12.3 EnCore (Ensuring Consent and Privacy)</td>
<td>50</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.12.4</td>
<td>PV Nets (Privacy Value Networks) 2008-2011</td>
<td>50</td>
</tr>
<tr>
<td>2.12.5</td>
<td>VOME (Visualisation and Other Methods of Expression) 2008-2012</td>
<td>52</td>
</tr>
<tr>
<td>2.12.6</td>
<td>RISE (Rising pan-European and Internal Awareness on Biometrics and Society Ethics)</td>
<td>53</td>
</tr>
<tr>
<td>2.13</td>
<td>Societal Implications of Implementing this Technology</td>
<td>54</td>
</tr>
<tr>
<td>2.14</td>
<td>Legal Implications</td>
<td>63</td>
</tr>
<tr>
<td>2.14.1</td>
<td>The Legal Right to Privacy</td>
<td>65</td>
</tr>
<tr>
<td>2.14.2</td>
<td>The Diffusion Effect</td>
<td>67</td>
</tr>
<tr>
<td>2.14.3</td>
<td>Implications of the Data Protection Act 1998</td>
<td>71</td>
</tr>
<tr>
<td>2.14.4</td>
<td>The Retention of Data and Civil Liberties</td>
<td>73</td>
</tr>
<tr>
<td>2.14.5</td>
<td>The Retention of DNA Samples</td>
<td>76</td>
</tr>
<tr>
<td>2.15</td>
<td>Ethical Implications and the Impact of Computer Ethics</td>
<td>78</td>
</tr>
<tr>
<td>2.16</td>
<td>Impact of Social Exclusion</td>
<td>83</td>
</tr>
<tr>
<td>2.17</td>
<td>Theories for Conceptual Framework</td>
<td>86</td>
</tr>
<tr>
<td>2.18</td>
<td>Chapter Summary and Conclusions</td>
<td>90</td>
</tr>
</tbody>
</table>

### Chapter 3: The Conceptual Framework

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>93</td>
</tr>
<tr>
<td>3.2</td>
<td>The Research Path</td>
<td>93</td>
</tr>
<tr>
<td>3.2.1</td>
<td>The Ontological Perspective of the Social Constructionist</td>
<td>94</td>
</tr>
<tr>
<td>3.2.2</td>
<td>The Epistemological Perspective of Interpretivism</td>
<td>95</td>
</tr>
<tr>
<td>3.3</td>
<td>The Multi-model: Institutional Theory and Technology Acceptance Model</td>
<td>97</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Institutional Theory</td>
<td>98</td>
</tr>
<tr>
<td>3.3.2</td>
<td>The Technology Acceptance Model</td>
<td>99</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Advantages and Disadvantages of the Model</td>
<td>99</td>
</tr>
<tr>
<td>3.3.4</td>
<td>Practical Application of the Technology Acceptance Model</td>
<td>100</td>
</tr>
<tr>
<td>3.4</td>
<td>Framework for Investigation</td>
<td>100</td>
</tr>
<tr>
<td>3.4.1</td>
<td>The Utilitarian Philosophy (applicable to Management and Workforce)</td>
<td>101</td>
</tr>
<tr>
<td>3.4.2</td>
<td>Maslow’s Theory of Needs (applicable to the Workforce)</td>
<td>104</td>
</tr>
<tr>
<td>3.4.3</td>
<td>The Psychological Contract (applicable to Management and Workforce)</td>
<td>108</td>
</tr>
<tr>
<td>3.5</td>
<td>Application of Theoretical Perspectives to Research Objectives</td>
<td>111</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Approach to Case Studies</td>
<td>112</td>
</tr>
<tr>
<td>3.5.2</td>
<td>The Cases</td>
<td>115</td>
</tr>
<tr>
<td>3.5.3</td>
<td>Risks Emerging from the Interview Process</td>
<td>119</td>
</tr>
<tr>
<td>3.6</td>
<td>Chapter Summary and Conclusions</td>
<td>124</td>
</tr>
<tr>
<td>Chapter 4: Research Approaches (Actualisation)</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>4.1 Introduction</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>4.2 Choosing an Appropriate Unit if Analysis</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>4.3 The Use of Multiple Embedded Case Studies</td>
<td>129</td>
<td></td>
</tr>
<tr>
<td>4.4 Case Study Design</td>
<td>133</td>
<td></td>
</tr>
<tr>
<td>4.5 Advantages and Disadvantages of the Case Study Approach</td>
<td>136</td>
<td></td>
</tr>
<tr>
<td>4.6 The Concept of “Best Practice”</td>
<td>136</td>
<td></td>
</tr>
<tr>
<td>4.7 Piloting</td>
<td>137</td>
<td></td>
</tr>
<tr>
<td>4.7.1 The Pilot Case Study: Sagem Securite (Basingstoke)</td>
<td>137</td>
<td></td>
</tr>
<tr>
<td>4.7.2 Statement of Purpose</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>4.7.3 Extract from Pilot Interview and Participant Responses</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>4.8 Concluding Comments on Pilot Interview</td>
<td>145</td>
<td></td>
</tr>
<tr>
<td>4.9 Chapter Summary and Conclusions</td>
<td>146</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5: Identification and Presentation of Current Practice</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Introduction</td>
<td>149</td>
</tr>
<tr>
<td>5.2 The Case Study Selection Process</td>
<td>149</td>
</tr>
<tr>
<td>5.3 The Interview Transcription and Editing Process</td>
<td>150</td>
</tr>
<tr>
<td>5.4 Case Study A</td>
<td>151</td>
</tr>
<tr>
<td>5.4.1 Semi-structured Interview with Management</td>
<td>152</td>
</tr>
<tr>
<td>5.4.2 Semi-structured Interviews with Workplace Participants</td>
<td>155</td>
</tr>
<tr>
<td>5.5 Case Study B</td>
<td>158</td>
</tr>
<tr>
<td>5.5.1 Semi-structured Interview with Management</td>
<td>159</td>
</tr>
<tr>
<td>5.5.2 Semi-structured Interviews with Workplace Participants</td>
<td>163</td>
</tr>
<tr>
<td>5.6 Case Study C</td>
<td>165</td>
</tr>
<tr>
<td>5.6.1 Semi-structured Interview with Management</td>
<td>166</td>
</tr>
<tr>
<td>5.6.2 Semi-structured Interviews with Workplace Participants</td>
<td>169</td>
</tr>
<tr>
<td>5.7 Case Study D</td>
<td>175</td>
</tr>
<tr>
<td>5.7.1 Semi-structured Interview with Management</td>
<td>175</td>
</tr>
<tr>
<td>5.7.2 Semi-structured Interviews with Workplace Participants</td>
<td>180</td>
</tr>
<tr>
<td>5.8 Chapter Summary and Conclusions</td>
<td>187</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Chapter 6: Analysis of Best Practice and Development of “Best Practice” Model</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Introduction</td>
<td>189</td>
</tr>
<tr>
<td>6.2 Suggested “Best Practice” Model</td>
<td>189</td>
</tr>
<tr>
<td>6.3 Application of Suggested Model to the Selected Samples</td>
<td>191</td>
</tr>
<tr>
<td>6.4 Presentation and Analysis of feedback from representatives Of (Case Study A and Case Study C)</td>
<td>193</td>
</tr>
<tr>
<td>6.4.1 Background</td>
<td>193</td>
</tr>
<tr>
<td>6.4.2 Participant Responses and Analysis (Case Study A and Case Study C)</td>
<td>193</td>
</tr>
<tr>
<td>6.5 Presentation of Suggested “Best Practice Model” Emerging from representatives of the Selected Samples (Case Studies A and C)</td>
<td>205</td>
</tr>
<tr>
<td>6.6 The Model</td>
<td>205</td>
</tr>
<tr>
<td>6.7 Recommendations for Best Practice Responding to Elements of Social, Legal and Ethical Considerations in the Management of Biometric Access Control Systems</td>
<td>206</td>
</tr>
<tr>
<td>6.8 Chapter Summary and Conclusions</td>
<td>210</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7: Conclusions and Recommendations for Further Research</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Introduction</td>
<td>212</td>
</tr>
<tr>
<td>7.2 Major Findings: Answers to Research Question</td>
<td>213</td>
</tr>
<tr>
<td>7.3 Contributions to Theory, Practice and Methodology</td>
<td>218</td>
</tr>
<tr>
<td>7.4 Limitations of this Study</td>
<td>222</td>
</tr>
<tr>
<td>7.5 Opportunities for Further Research</td>
<td>225</td>
</tr>
<tr>
<td>7.6 Personal Reflections</td>
<td>290</td>
</tr>
</tbody>
</table>

i. Appendices viii
ii. Table of Figures ix
iii. Abbreviations x
iv. References and Bibliography 228
Appendices

Appendix 1: Application form for Ethics Approval

Appendix 2: Sample Semi-structured Interview and Transcript of Pilot Case Study

Appendix 3: Semi-Structured Interview with Management

Appendix 4: Semi-Structured Interviews with Workplace Participants

Appendix 5: Suggested Best Practice responding to the Social, Legal and Ethical perceptions of Biometric Access Control Management [Case Study A]

Appendix 6: Suggested Best Practice responding to the Social, Legal and Ethical perceptions of Biometric Access Control Management [Case Study C]
<table>
<thead>
<tr>
<th>Figure 1:</th>
<th>Research Path</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 2:</td>
<td>Conceptual Framework</td>
<td>97</td>
</tr>
<tr>
<td>Figure 3:</td>
<td>Choosing the Unit of Analysis</td>
<td>128</td>
</tr>
<tr>
<td>Figure 4:</td>
<td>Multiple Case Studies</td>
<td>135</td>
</tr>
</tbody>
</table>

 ix
Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFIS</td>
<td>Automated Fingerprint Identification System</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>BCS</td>
<td>British Computer Society</td>
</tr>
<tr>
<td>BSI</td>
<td>British Standards Institute</td>
</tr>
<tr>
<td>BSIA</td>
<td>British Security Industry Association</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>CFET</td>
<td>Computer Forensics Education and Training</td>
</tr>
<tr>
<td>CNIL</td>
<td>Commission Nationale de l’Informatique</td>
</tr>
<tr>
<td>CONI</td>
<td>Cabinet Office and the Centre for National Infrastructure</td>
</tr>
<tr>
<td>CRB</td>
<td>Criminal Records Bureaux</td>
</tr>
<tr>
<td>DART</td>
<td>Dynamic Acceptance Model for the Re-evaluation of Technologies</td>
</tr>
<tr>
<td>DNA</td>
<td>Deoxyribonucleic Acid</td>
</tr>
<tr>
<td>DSO</td>
<td>Departmental Security Officer</td>
</tr>
<tr>
<td>DTI</td>
<td>Department of Trade and Industry</td>
</tr>
<tr>
<td>DV</td>
<td>Defence Vetting</td>
</tr>
<tr>
<td>EC</td>
<td>European Community</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>En CORE</td>
<td>Ensuring Consent and Privacy</td>
</tr>
<tr>
<td>EPSRC</td>
<td>Engineering and Physical Sciences Research Council</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>GMAC</td>
<td>Graduate Management Council</td>
</tr>
<tr>
<td>HO</td>
<td>Home Office</td>
</tr>
<tr>
<td>ICT</td>
<td>Information Communication Technology</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>IPA</td>
<td>Interpretative Phenomenological Analysis</td>
</tr>
<tr>
<td>IRA</td>
<td>Irish Republican Army</td>
</tr>
<tr>
<td>IT</td>
<td>Institutional Theory</td>
</tr>
<tr>
<td>LSPI</td>
<td>Legal Security and Privacy Issues</td>
</tr>
<tr>
<td>LLM</td>
<td>Master of Laws</td>
</tr>
<tr>
<td>MA</td>
<td>Master of Arts</td>
</tr>
<tr>
<td>MOD</td>
<td>Ministry of Defence</td>
</tr>
<tr>
<td>MTAS</td>
<td>Material Transfer Agreement Standard</td>
</tr>
<tr>
<td>NAFIS</td>
<td>National Associated Fingerprint Biometric System</td>
</tr>
<tr>
<td>NASP</td>
<td>National Aviation Security Policy</td>
</tr>
<tr>
<td>NEC</td>
<td>National Exhibition Centre</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PETS</td>
<td>Privacy Enhancing Technologies</td>
</tr>
<tr>
<td>PINS</td>
<td>Personal Identification Numbers</td>
</tr>
<tr>
<td>PITO</td>
<td>Police Information Technology Organisation</td>
</tr>
<tr>
<td>PV Nets</td>
<td>Privacy Value Networks</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
</tbody>
</table>
RISE
Rising pan-European and International Awareness on Biometric and Security Ethics

SAS
Strong Authentication Service

SEAP
Security Environment Assessment Panel

TAM
Technology Acceptance Model

UID
Unique Identification

UKPS
United Kingdom Protection Services

UWIC
University of Wales Institute, Cardiff

VOME
Visual and Other Methods of Exposure

3D
Three-dimensional

2D
Two-dimensional
Chapter One

Introduction to the Investigation
1.1 Introduction

This thesis investigates the social, legal and ethical implications of biometric technology represented by fingerprint scanning and facial recognition systems in a sample of United-Kingdom based organisations. It focuses on an assessment of management strategies and workforce perceptions towards the use of this technology for access control within specific workplace environments, following a series of security risks emerging from the early millennium. Primary and secondary perceptions of key players in the area of biometric applications have been reviewed and their perceptions represented by practitioners in the access control environment and representatives of the United Kingdom Border Agency. Their considered opinions led to the conclusion that fingerprint and facial recognition systems in particular, should be considered before general assumptions can be made about the effects of more recent biometric technologies. Consequently this investigation focuses on the application and management of fingerprint scanning and facial recognition technology for access control.

The research path focuses on a discrete sample of United Kingdom based organisations, using a combination of Utilitarianism propounded by John Stuart Mill, Abraham Maslow’s Hierarchy of Needs and the concept of the Psychological Contract. This has led to the development of a series of Recommendations for Best Practice in applying social, legal and ethical approaches to engendering acceptance of biometric technology in the workplace. A qualitative paradigm is used in which four case studies are considered in detail with content analysis from interviews with representatives of management and workforce.
1.2 Background

Mordini and Petrini (2007: 5) defined biometrics as: "a generic word which relates to the systematic presentation of quantitative studies concerning life phenomena."

Biometric technology has also been referred to as the measurement of physiological characteristics such as fingerprints, facial recognition and hand geometry, distinctive to an individual. In addition, the technology applies to behavioural characteristics such as voice, signature or keystroke recognition (Sloan Coats et al., 2007). It has traditionally been used to establish physical and difficult to alienate characteristics, including appearance, social behaviour or natural physiology, based on a metric or measurement.

This investigation considers the implementation and management of biometric technologies for access control in a selection of United-Kingdom based organisations. They represent Local Government, a Business College catering for one hundred percent overseas students, a Public Communications organisation and a representative of the Aviation industry.

1.3 Scoping the Research

The parameters for the investigation are based on the security alerts emerging from the attack on the World Trade Centre in September 2001. This event is considered to have formed a catalyst for the application of biometric technology to safeguard current day security. The research undertakes primary and secondary perceptions of key players in the field of biometric applications, with initial (pilot) participants including Practitioners in access control environments and representatives of the United Kingdom Border Agency. Their perceptions led the investigation to focus on fingerprint scanning and facial recognition systems, before purporting to arrive at general assumptions about the effects of the more recently emerging (bleeding edge) technologies.

The theoretical foundation for this investigation is built on a combination of "Institutional Theory" and the "Technology Acceptance Model". The former considers
the structures, rules and norms established by organisations and how they are responded to in aspects of social behaviour (Scott, 2004). The latter determines the process by which the implementation of biometric technology may be accepted by workplace members (Dimitriadis, 2006).

The conceptual framework focuses on a combination of the Utilitarian principle enunciated by John Stuart Mill, Abraham Maslow’s Hierarchy of Needs and the concept of the Psychological Contract. This combination of theoretical and conceptual frameworks leads to the development of a series of Recommendations for “Best Practice” in fostering workplace acceptance of (selected) biometric technologies used for access control.

The scope of the investigation underwent final refinement following attendance at the IFSEC Global Information Security conference at the National Exhibition Centre (NEC), Birmingham in March 2008. Representation from the United Kingdom Border Agency suggested that fingerprint scanning and facial recognition systems were likely to remain the bulwark for general security and border control for a substantial time. The ultimate decision to focus on these technologies was confirmed however, following a pilot study conducted in March 2009, where it was recognised that:

“Good quality samples of finger impressions are not the easiest to capture for manual workers so for such things as building sites or engineering works, we will probably see an increase in the use of hand geometry and / or vein together with facial recognition…..”, whilst it was considered that: “More and more schools, nightclubs, nurseries and health care applications are using fingerprints for access control,” (Preston, 2009).

It was the suggestion that fingerprint scanning and facial recognition systems are likely to remain trusted methods of access control in diverse areas of security management that confirmed the appropriate selection of technologies for this investigation.
1.4 The Research Problem and Question

This study reflects on social, legal and ethical guidelines for accessibility and privacy in the deployment of biometric systems (Sims, 2009). It focuses on a discrete sample of specific organisations using or considering the use of biometric technology for access control, in developing a series of recommendations to maximise social, legal and ethical acceptance, in answering the research question:

_How should organisations using biometric access control systems address social, legal and ethical concerns in the management of specific working environments in the United Kingdom?_

1.5 Justification for the Thesis

The thesis aims to balance national and international standards for the acceptable implementation of biometric access control, combining the Utilitarian principle (Harris, 1997) that legislation and other institutional constraints can be justified only, if they on balance promote general happiness. It also considers Maslow’s Hierarchy of Needs, suggesting that human beings are motivated by fulfilling unsatisfied needs and that lower level needs must be satisfied before considering social and esteem needs. This is followed with the concept of the Psychological Contract, reflecting on how expectations change with time and technological development. This framework forms the basis for producing a series of recommendations to maximise the social, legal and ethical acceptance of biometric technology in the organisations under investigation.

The investigation has used an embedded case study approach, in recognising the need for management to balance the legal demands to control their sensitive and safety critical data with the social, legal and ethical concerns of their workforce (Yin, 2009)
1.6 The Research Agenda

The agenda has been prepared objectively from the point of allocated tasks but in terms of deadlines set for each, it is recognised (Blaxter et al., 2002) that the time any particular research activity will take should not be under-estimated. The schedule has been re-visited regularly and amendments have been made to reflect the necessary flexibility and to ensure that the research activities are monitored closely for tracking purposes (refer to Figure 1: Research Path (overleaf)).
Objectives

Research Aim (statement of intention) - Investigation

Biometric Technology for Access Control for Workplace Management

Literature Review (biometric access control & social, legal, ethical implications & standards)

Conceptual Framework

Utilitarianism, Need, Psychological Contract (Institutional Theory & Technology Acceptance Model)

Methodology (Multiple Case Studies)

Experts in Social, Legal and Ethics

CARDIFF INT. AIRPORT, WAG, BT, BARNET COLLEGE

Figure 1: Research Path
1.7 Aim and Key Objectives:

1.7.1 Aim

The thesis aims:

To compile a series of Recommendations for "Best Practice" to maximise the social, legal and ethical acceptance of biometric technology for access control management in a sample of United Kingdom-based organisations.

1.7.2 Key Objectives

The objectives focus on investigation, implementation and reflection:

1. To investigate the development and perception of biometric technology involving fingerprint scanning and facial recognition systems for access control to workplace environments, by means of a critical literature review.

2. To assemble representative case studies, combining the conceptual frameworks of Utilitarianism, Needs and Psychological Contract by undertaking semi-structured interviews with management.

3. To compile an audit of current practice, involving a series of semi-structured interviews with sample organisations. This involves collecting data and undertaking content analyses to focus on Utilitarianism, Needs and the Psychological Contract within the context of biometric access control.

4. To synthesise empirical investigation towards the development of a first-cut series of recommendations to maximise the acceptance of biometric access control. This process uses examples of best practice generated from secondary and empirical studies, using semi-structured interviews with participant organisations. It focuses on participants' perceptions of Needs in responding to biometric access control and the impact of the Psychological Contract.
5. To generate and disseminate a working series of Recommendations for consideration and feedback, and

6. To evaluate links between primary and established responses, using semi-structured interviews with a selection of management and workforce. This objective uses a process of Content Analysis in developing a series of Recommendations for “Best Practice” based on theories of Utilitarianism, Needs and the Psychological Contract.

1.8 Research Methods

The process begins with a review of the literature associated with biometric technology for access control and its implementation within working environments. This is followed by the choice of an inductive method to develop theories from abstract concepts (Creswell, 2007). Fieldwork is undertaken using a combination of Social Constructionist and Interpretivism approaches.

This strategy focuses on linking ontological and epistemological perspectives to establish “meaning” within the investigation (Silverman, 2007). A series of semi-structured interviews have been conducted with management and workplace representatives. Individual perceptions have been reviewed using a process of content analysis, involving coding, annotating and setting time aside between the collection and analysis of data, towards “defogging” a foggy research issue (Miles and Huberman, 2007).
1.9 Chapter Summary and Conclusions
This chapter has introduced the investigation into management strategies towards the social, legal and ethical application of biometric technology. It has made reference to fingerprint scanning and facial recognition systems, in a sample of United Kingdom-based workplace environments. The chapter has reflected on social, legal and ethical guidelines for accessibility and privacy in the deployment of biometric systems, whilst referring to the application of guidelines for specific organisations using biometric technology for access control. Reference has been made to the development of a series of recommendations to maximise social, legal and ethical acceptance in addressing the research question:

*How should organisations using biometric access control systems, implement procedures to address social, legal and ethical concerns in the workplace management of specific environments in the United Kingdom?*

1.10 Summary of Subsequent Chapters
The following represents a summary of the subsequent chapters underpinning this thesis.

1.10.1 Chapter Two: Literature Review
series of associated Engineering and Physical Sciences Research Council (EPSRC) funded projects with social, legal and ethical implications.

1.10.2 Chapter Three: The Conceptual Framework

This chapter discusses the ontological and epistemological perspectives represented by Social Constructionism and Interpretivism together with the dual principles of Institutional Theory and Technology Acceptable Models. It considers this multi-model approach as forming the basis for arriving at a conceptual framework in which principles of Utilitarianism, Needs and the Psychological Contract are applied to both management and workforce.

1.10.3 Chapter Four: Research Approaches (Actualisation)

Chapter Four considers the unit of analysis chosen for the investigation, discussing the use of multiple-embedded case studies, in which semi-structured interviews have been conducted across a range of organisations, with representatives of management and workforce. The chapter also discusses the advantages and disadvantages of the case study approach, concluding that well designed case study data (incorporating appropriate structure and piloting) results in the effective testing of concepts and theories in their natural environment.
1.10.4 Chapter Five: Identification and Presentation of Current Practice

This chapter identifies the case study participants selected for the investigation. It clarifies the rationale and background of each case and discusses the processes for interviewing management and workplace participants. The primary consideration for identifying a suitable sample was based on the extent to which selected organisations would be representative of the topic under investigation. Chapter five justifies the choice of the sample having been selected, by balancing a representative number of organisations with a manageable sample for investigation, to arrive at objectively defensible reasons for social, legal and ethical perceptions of this technology.

1.10.5 Chapter Six: Development of “Best Practice” Model

This penultimate chapter defines the general concept of “Best Practice” in developing a series of recommendations for implementing biometric access control procedures within the case studies under investigation. It clarifies this process as having led to the development of a (first-cut) series of suggestions being sent to a sample of respondents selected from Case Studies A and C for consideration, comment and assimilation of suggested “Best Practice.”

1.10.6 Chapter Seven: Conclusions and Recommendations for Further Research

This final chapter undertakes a review of the aims and objectives set for the thesis and reviews each objective. This has led to a re-statement of the major findings arising from the empirical investigation within Cases A, B, C, and D. The chapter reflects on the conceptual framework represented by the Institutional Theory and Technology Acceptance Models set within the parameters of Utilitarianism, Needs and the Psychological Contract. It focuses on six (extracted from twelve) of the controls contained within ISO/IEC 27002 Information Technology – security techniques – Code of Practice for Information Systems Management towards the development of “Best
Practice" for social, legal and ethical acceptance of (selected) biometric technology for access control within the samples investigated. The chapter concludes with reference to practical limitations and opportunities for further research in this area, whilst reflecting on the personal experiences of the research process.
Chapter Two

Literature Review
2.1 Introduction


Having undertaken a critical review of the available literature this chapter proceeds to identify the theories incorporated into the conceptual framework for investigation. Theories are based on the ontology of Social Constructionism and the epistemology of Interpretivism. They rest on the dual foundation of Institutional Theory and the Technology Acceptance Model in applying principles of Utilitarianism, Maslow’s Hierarchy of Needs and the Psychological Contract.

2.2 DNA Sampling, Biometric Technology and the Perceived Threat to Civil Liberties

DNA (deoxyribonucleic acid) or the hereditary material present in human and all other organisms is located in the cell nucleus as representing the specific order or blueprint in the construction of cells. This is the genetic code enabling organisms to read the information contained within specific genes, representing heredity in human organs (Nguyen et al., 2002). The information security environment is constantly searching for more efficient methods of ensuring encryption towards the development of un-breakable algorithms, to secure a position in which biometric identification is recognised as the most secure method of establishing reliable identification techniques. This dichotomy has led to discussion about the links forged between DNA and biometric identification, in which a strategy has been proposed in which personal medical data is encrypted in DNA strands, based on a central platform of molecular biology. The proposal is that the
blood mineral levels of an individual is used as a process for selecting, transmitting and recovering the “public key” associated with that individual (Vaida et al., 2006).

This linking process has been considered further by the United States Department of Defense in its tracking process for both known and unknown (recognisable and unrecognisable) personnel for purposes of identity management. In this context again, the link between biometrics and DNA sampling in the process of identity management has been recognised. Here emphasis is placed on the unique and untraceable nature of DNA but the viability of using DNA as a biometric is continually under investigation, for purposes of securing civil liberties. Conversely, whilst any biometric identification system is likely to represent a threat to civil liberties with the risk of all human behaviour becoming transparent to the State, there is evidence of individuals being prepared to relinquish civil liberties when they fear for their personal security. Don and Davis (2001) suggested that there was relative American ambivalence towards security following the attacks on the World Trade Centre in New York on September 11th 2001. This led to half of the New Jersey residents surveyed by Newark Star-Ledger, recording no objection to the authorities monitoring phone calls or email messages, and 70% of participants reporting a belief that Americans would have to give up some personal freedom for national security.

Sloan Coats et al., (2007) suggested that the events of September 11th 2001 also led to increased calls for biometric identification systems worldwide. But, despite fingerprint and iris scanning technology recognised as having the potential to strengthen security, practical questions have arisen about the effects of Government and Corporate databases registering and storing this data. Piper (2004) had suggested that the key to preserving personal identity does not rest with biometrics itself but with ensuring that the initial registration system is accurate. In response to this, Sloan Coats et al., (2007) argued that no method of identification or verification is foolproof and no single technology can guarantee security. But despite biometric identifiers not being infallible, they are increasingly recognised as having the potential to enhance security and to date, perhaps they represent the most accurate identification process available. Their uniqueness in identification also means that the difficulty of forging biometric identity
has deterred identity thieves who may have traditionally experienced little difficulty in spoofing personal papers and cards.

Conversely, the Nuffield Council on Bioethics, in its Executive Summary of The Forensic Use of Bio-information 2007, suggested that there are practical concerns with both fingerprint scanning and DNA profiling, despite their increasing robustness and reliability. Chapter Two of this Report suggested that risks may arise from deliberate or accidental mixing and mis-matching of samples, leading to contamination and misinterpretation. In response, the interpretation of bio-information contained in Chapter Three of the Report entitled: “Ethical Values and Human Rights” emphasised the importance of proportionality by the State in ensuring that rights and values based on liberty, privacy and informed consent are preserved.

In the area of criminal investigation, the Nuffield Report (2007) recognised proportionality in the taking of fingerprint and biological samples following arrest in connection with a recordable offence without the consent of the suspect. But it was more sceptical of Home Office proposals in March 2007, that the police be permitted to take and store fingerprints and biological samples from all arrestees, irrespective of the status of the offence, (Nuffield Council on Bioethics, 2007). Further concerns surrounded the retention of biometric samples, with the Nuffield Report (2007) highlighting different approaches in the United Kingdom and the rest of Europe and between the United Kingdom and Scotland. The Criminal Justice Act 2003 extended the retention of fingerprinting and biological samples indefinitely in cases of arrest for recordable offences and the Home Office proposals in March 2007 had extended this to all arrestees, irrespective of conviction. In Scotland such retention is only available upon conviction, and for three years, irrespective of conviction, when the charge relates to a serious violent or sexual offence.

There are specific concerns surrounding the retention of bio-information, particularly those relating to the over-representation of black and ethnic groups and the number of records relating to minors on bio-information Databases (Nuffield Council on Bioethics, 2007, Executive Summary: xvii) This represents more serious implications in the
United Kingdom as opposed to other European countries, with the United Kingdom criminal age of responsibility at age ten, and the Scottish system lower still, at age eight. The report suggested that the retention of such information from young people contravenes Article 40 of the United Nations Convention on Human Rights of the Child 1990. It pointed to the requirement to provide special legal protection to young children to guard against stigma and to provide rehabilitation opportunities to those who have offended. The Information Commissioner for the United Kingdom asked that schools seek consent from parents before taking pupils’ fingerprints, despite there being no legal obligation to do so (Ballard, 2007).

There is a gap here between law and ethics, in that as Ballard (2007) suggested, the Data Protection Act 1998 makes no legal provision for gaining consent so there is no established sanction but the requirement for parental consent is based on social and ethical indicators enunciated by best practice. Ballards’s (2007) article made reference to the Gillick precedent that minors can make their own judgement about data protection when they reach maturity. However this had led to a complicated debate about the age at which a child could be socially deemed to understand the nature of informed consent. Ages have ranged from twelve to sixteen in discussions between the Information Commission Office and representatives of Action Rights on Children, where further issues have arisen as to what a minor may understand about the nature of the information being shared. For example, s/he may raise no objection to data being shared about his or her dyslexia but may wish to resist information being shared about family status and associated issues.

2.3 Perceived Benefits of Biometric Technologies

Despite concerns having been raised about the impact of this technology on civil rights, a number of socially advantageous implications of biometrics have been recognised. Woodward (2002) alluded to the extensive use of biometrics for human recognition from both public and private sectors. He suggested that whilst the technology may pose legitimate threats to privacy, concerns can be addressed with carefully considered social, legal and ethical strategies. He further suggested that biometric technology has the potential to develop into a socially accepted phenomenon in which it is recognised
as an advocate of privacy. This led to the conclusion that social acceptance of biometrics rests with society’s perception of its value to individuals within their environments, weighed against perceived risks of social intrusion and invasion of privacy.

Howarth (2005) supported Woodward (2002) suggesting that one of the most critical objections rests with individuals’ fears that information gathered could be used to produce records to track social habits and lifestyles. She further suggested that such information could be used to target specific social groups and that this has led to general scepticism. In this respect, Howarth’s (2005) argument parallels that of the Silicon assessment of Biometrics (2007), with the latter suggesting that people accept this technology only to the extent that it has perceived benefits for society as a whole.

Howarth (2005) further suggested that whilst biometric technology may be socially acceptable for air travel and using Automatic Teller Machine (ATM) facilities, it is often less acceptable in areas of perceived social intrusion such as for logging on to personal computers in a workplace setting. Howarth (2005) further suggested that, on questions of security and functionality of biometric systems, social concerns about the risk of losing data from databases led people to favour smart cards for storing biometric information.

### 2.4 Fingerprint Recognition

Jain et al., (1999) had perceived this technology as having an established history, emerging from use in clinical investigations for the identification of individuals and from the capturing of prints with ink and paper to its current status in which digitized data is translated into two major algorithms (minutiae and pattern). Later, Johnson (2005) pointed to sensor designs (optical, ultrasonic, passive and active capacitance), compared against databases in real time, as representing what scientists believe to be inherited arch, loop and whorl patterns and minutiae. He suggested that no two fingers, even in identical twins, have been shown to be identical.
The quality of the image may be compromised by a scratched or dirty touch surface and by the condition of the fingerprint, represented by dirty or worn fingers, leading to the requirement of live finger detection within the system. But Jain (1999) and Johnson (2005) suggested that the need for clean, undamaged skin is eliminated by the use of ultrasonic sensors to capture fingerprint images, using high frequency and sound waves to penetrate the epidermal skin layer. In this case a passive capacitance sensor forms an image of the fingerprint pattern on the dermal layer. Measurements are taken between ridges and valleys at the point where the dermal layer and sensing element in valleys produces air gaps so that capacitance values can distinguish between ridges and valleys in fingerprints by following the pattern of ridges in the dermal layer. In support of this, Mazumdar et al., (2008) considered the voltage from the dermal layer and sensing element and compared them against a reference voltage to calculate capacitance, using a match formulation to form an image of the finger. This used the principle of ultrasonic measurement, eliminating the need for clean, undamaged fingerprints.

This process of matching had been further considered by Mazumdar et al., (2008) in their White Paper published in 2003, entitled: "Minutia vs Pattern Based Fingerprint Templates". The research had suggested that algorithms may also be used to capture previously stored and current or real time templates by finding a central point in the finger image to align the two images in the same orientation. This would contain the type, size and orientation of patterns within aligned prints, allowing for the degree of match or miss-match to be calculated by graphical comparison.

### 2.5 Facial Recognition

This technology developed from the Automated Facial Recognition techniques introduced by Woody Bledsoe, Helen Chan-Wolf and Charles Bisson during 1964 and 1965, using computers to recognise human features, but their research was funded by an anonymous agency, prohibiting the publication of many of its findings. This research had focused on the selection and matching of a small set of records from a large database of photographs. The process was criticised by Bledsoe, however, (1966) as
being complicated by the great variation in head rotation and tilt, lighting intensity and angle, facial expression and the ageing process.

Blesdoe (1966) argued that the method of correlation (or pattern matching) is certain to fail in cases where the variability is great. In particular, he pointed to the correlation being very low between two pictures of the same person with two different head rotations. In contrast, more recent research has shown that despite increasing use of cosmetic surgery, facial features remain identifiable from birth to death (Herbert, 2001). But from the perspective of identification, facial recognition requires a large image, using clear lighting conditions and that it is most suitable for system authentication at fixed locations, such as at access control points.

Bonsor (2008) suggested that recognition is usually sustained from an algorithm used to analyse the relative positioning of facial features including the shape of the nose to eyes in relation to the jaw or cheekbone (the facial triangle) used to search for matching images. The algorithms are divided into two main approaches, representing geometric or ordinary features and photometric or a statistical means of distilling images into mathematical values, using templates to eliminate points of variance.

Kepler (2004) also pointed to three-dimensional (3D) sensor processes having been used to identify distinctive facial features from nose shape and depth to eye socket and jawbone formulation. He suggested that this process has the advantage of identifying facial features from a profile, irrespective of external quality of lighting and other location distractions. Whilst he alluded to potential compromise arising from differences in facial expression and subsequent analysis; Kepler (2004) suggested that this risk to validity has been responded to by metric geometry applied to treat expressions as isometrics. Whilst Psillos and Al-Dabass (2008) pointed to other available techniques stemming from skin texture analysis in which facial blemishes are translated into mathematical space having the capacity to increase representations of accuracy by 20-25%.
Reliability is a main consideration in areas of security management, but despite this Shoniregun (2004) suggested that one of the main practical advantages of facial recognition is that there is no requirement for consent to capture an image. A number of United Kingdom-based organisations have used this technology to good effect in security areas, with the London Borough of Newham having trialled facial recognition in its borough-wide CCTV system from 2004. But critics of the system suggested that since its inception, Newham’s automatic facial recognition system has not spotted a live target. This contradicts the Borough’s claim that the system has led to a 34% reduction in crime in the area, leading to the roll-out of a similar system in Birmingham (Shoniregun, 2004).

On the wider question of accuracy and reliability, Phillips et al., (2006) referred to results gained from the Face Recognition Grand Challenge in 2006 in which high resolution facial images and 3D face scans were used simultaneously with iris images. This reported facial technology as being ten times more accurate than that assessed in 2002 and one hundred times more accurate than that of 1995. Indeed, Phillips et al., (2006), in comparison with the contention of Johnson (2005) suggested that some algorithms revealed the potential to uniquely identify identical twins and to out-perform human recognition.

Taking a more measured approach however, Song et al., (2009) suggested that each pattern has individual advantages and disadvantages for security. They agreed with Johnson (2005) that considerable research has recognised that face and fingerprint recognition is non-intrusive, despite its inability to provide precise identification in certain circumstances, specifically in the recognition of twins and in the area of fingerprints, whilst pore features are recognised as being permanent and unique for forensic applications. They also suggested that sweat pores in faces are influenced by facial expressions and blemishes.

In overall assessment of reliability, Song et al., (2009) suggested that beyond fingerprint and facial recognition that of nose pores is clearer. They satisfy the biometric requirements of universality, distinctiveness, permanence and collectability all essential
features in addressing social, legal and ethical concerns about the reliability and choice of biometric application. However, Bogart (2008) suggested that fingerprint technology will continue to dominate for access control readers and laptops, with readers being developed in conjunction with personal identification numbers, proximity, smart cards and tokens. Bogart (2008) considered this multiplicity of approach as important in ensuring strong international authentication and access control. He pointed specifically to its application in mobile devices with the progressive use of smart phones operating as a gateway to confidential information.

Bogart (2008) referred to facial recognition as the second most widely deployed technology internationally after fingerprint. He suggested that this is recognised by the International Biometric Group as having the capacity to grow exponentially for the next ten years. He pointed to three-dimensional (3D) facial technology. This forms a valuable contingency to fingerprint scanning for access control when workers' hands are full or accuracy may be compromised by worn or dirty fingers, rendering it more generally acceptable for mainstream users.

Whilst fingerprints have an established history for biometric applications as part of the solution to identification, more recently palm print identity has also been used worldwide, specifically in the banking sector. This technology, together with palm vein and facial recognition, have increased in significance to deal with identification fraud, but from the point of general social acceptance, Skinner (2010) suggested that on balance, facial recognition has been favoured in China, specifically for purposes of the Beijing Olympics due to its non-intrusive character, raising fewer social objections. In addition, facial recognition has been recognised as rarely presenting false positive or false negative results. And its potential to scan more than a million faces in fewer than three seconds using a standard computer has increased its efficiency and effectiveness within access control environments.

Berrong (2010) also pointed to the sustained significance of fingerprint and facial recognition technology in European border control and within the construction of the Olympic Park in London. He referred to the annual Unysis Security Index and review of
consumer surveys in nine countries including Germany, the United Kingdom, Belgium, Spain and the Netherlands. This had suggested that consumers recognise security risks from terrorism and identity fraud towards sustained acceptance of biometric technology, from fingerprint and facial recognition to iris and retina scanning.

Whilst approximately 80% of biometric applications arise from government bodies, Berrong (2010) suggested that United Kingdom legislation regulating the provision of Health and Safety has encouraged increasing numbers of companies (especially those within the construction industry) to apply this technology in the authentication of specific personnel to sites. Berrong (2010) further pointed to the increased need for companies using biometric applications to ensure that they comply with the privacy requirements of the Data Protection legislation throughout the European Union. He stressed the importance of management awareness of the different privacy rules applicable, pointing to the stricter regulations in Germany and France, where biometric applications must be proportionate to the risk encountered, to be legally acceptable.

Berrong (2010) referred to fingerprint recognition being effectively prohibited in commercial applications in France, where the regulatory authority Commission Nationale de L’informatique et des Libertes (CNIL) insist on considering whether the proposed system is the most suitable for the defined purpose in relation to potential risks for personal data protection, compared with other potentially usable systems.

2.6 Universal Approaches to Fingerprint and Facial Recognition Systems

Arena and Cratty (2008) suggested that since the events of September 11th 2001, the United States Government has become aware of the increasing need to allocate funds towards developing a new form of biometric database to store DNA, fingerprints, eye scanning and tattoo mapping. And Frank (2007) pointed to the Department of Home and Security involvement in funding research into facial recognition systems. The Human Identification at a Distance program was capable of identifying facial features
up to a distance of five hundred feet. This process had been developed by the Information Processing Technology Office.

In contrast, the scanning of facial features at airports has been subject to privacy activists on questions of potential harm to civil liberties and risks of identification theft. This has highlighted United States and European concerns about the risks of criminals skimming facial features to identify citizenship remotely, for purposes of illegal tracking, stalking or kidnapping. Despite the risks identified, the United States Department of Defence issued a Common Access Card for identification relating to all service personnel and military sites, to catch biometric data and digitised photographs, and in the commercial environment, Walt Disney World was recognised to represent the nation’s largest commercial application of this technology until 2010, when the US-Visit Programme surpassed Disney biometric deployment in the United States. In Germany, Federal Government projects to develop fingerprint and facial recognition systems, increased from 12 million in 2004 to 377 million in 2009 (The Biometrics Market in Germany 2004-2009: Anti-terrorism Laws Drive Growth – Market Research Reports – Research and Markets) with the e. passport having been introduced containing a chip holding a digitised photograph and one finger from each hand.

This is usually represented by an index finger but capable of being inter-changed with other fingers where there is a risk of misreading from distorted fingerprints or missing fingers, with iris scans being a secondary consideration. (IDEBC-DE: Germany to phase in biometric pass ports from November 2005) The German approach is based on a culmination of ensuring the safety of citizens and complying with the United States waiver-visa, whilst introducing biometrics in passports. The fear of terrorist activity towards German athletes at the Olympic Games also intensified the German approach to this technology, based on the terrorist activity of 1972 when Germany held the Games in Munich, resulting in eleven Israeli athletes dying due to terrorist activity. The first use of biometric technology at a large-scale event of this nature took place at the Athens Olympics in 2004 where accredited visitors, were issued with identification cards containing their fingerprints.
The United States and German approaches to biometric technology have followed the South American lead with identification cards having been printed in Rio de Janeiro, since 2000. This contains a fully designed two-dimensional (2D) bar code incorporating information capable of being matched against the individual. This includes off-line encoding a colour photograph, signature and two fingerprints, collected during passport requests for storage in the ICADE Passport Standard in which an electronic image is generated to automatically recognise fingerprint templates and token facial images.

In the United Kingdom the Border Agency has recognised that despite the wide-ranging emergence of biometric security for access control, fingerprint and facial recognition systems are likely to remain the most “sustainable” with large-scale biometric applications for the foreseeable future. But social concern has been raised, most notably towards the use of this technology in schools. Issues have arisen from liberty groups about choices having been taken away from younger members of society. Concerns have also arisen about the potential for lack of privacy in data leakage and discrimination, where cases of means-testing for individual children is recorded and published.

Whereas in Germany and France, biometric applications to identify as opposed to verifying recognition would probably not be proportionate to risk in time and attendance, in the United Kingdom, there has been increased use of fingerprint recognition technology for time and attendance, due to its relative affordability Berrong (2010). The emphasis here rests with the need to comply with data protection laws by storing data on templates or cards as opposed to central storage devices.

More widely, a test case from the Mc Clean Virginia based Graduate Management Admission Council (GMAC) using fingerprint biometrics for security in a standard test for admission to many graduate business and management programmes worldwide since 1996, began from 2008 to consider biometric applications complying with international data privacy laws. It focused on “traceless technology” incapable of being captured without the subject’s knowledge, whilst being easily administered without the need for trained staff but with emphasis on universal subject acceptance. This led to
palm vein pattern recognition replacing GMAC’s fingerprint recognition system, in a 90 day pilot conducted in India and Korea, based on the relative accuracy of the former, whilst the latter is considered to degrade in time.

Berrong (2010) suggested that the result of the pilot was that most tests taken accepted palm vein technology, favouring its touch-less quality and perceived enhanced hygiene. This led to CNIL approval of GMAC’s use of palm vein technology in France from June 2009, in recognition of the relatively low risk of this technology for civil liberties and fundamental rights of the individual. There was support for its traceless character and insurance of subject knowledge supported with individual photographs and requirements for signature on a digital pad, stored on an encrypted digital template. And the assurance of central storage in the United States, where test takers’ names and test results are stored separately, led to its general acceptance (Berrong, 2010) using an encrypted algorithm.

2.7 Biometric Access Control for Workplace Management

Anderson (2008: 93) defined access control as:

"The meeting of security engineering and computer science to control which ‘principals’ (persons, processes and / or machines) have access to which resources: files, and programs that can be executed and how they can share data with other principals."

The traditional use of keys for access control within workplaces, has uncovered major flaws when large numbers have became unaccounted for and organisations have no system of collecting keys upon termination of an employee’s contract or the end of a contractual relationship. More recently, the concept of verifying the person as opposed to the access device has been favoured with the increased use of biometric access control systems. But despite fingerprint biometrics becoming more commonplace, questions have arisen as to the true level of its security (Dingle, 2008).
Social scepticism of this technology emerged in 2002-2003 with media revelations from Japanese research about fake prints being used from gelatine material in which "life checks" were scammed to measure pulse rate and perspiration on fingertips with latex material sufficiently fine for pulse rates to pass through, defeating life check security. At the same time, there were reported techniques using graphite powder and adhesive tape to lift fingerprints from surfaces, duping scanners into accepting their authenticity. Digital images would be enhanced on graphical software, printed on to foil. They would be transferred to a photosensitive circuit board; subsequently exposed to create a three-dimensional (3D) fingerprint for transfer to liquid latex, dried and transferred to a human finger, capable of scamming a biometric fingerprint reader.

In the context of computer science, biometric technology is used for two primary purposes, for access control management and to identify groups of individuals for surveillance purposes. Whilst the technology spans physical and behavioural traits, there are specific parameters to which most biometric technology is suitably linked. Jain et al., (2004) refer to the seven pillars of biometric uses, spanning but not limited to, human characteristics of uniqueness, permanence, ease of acquisition, accuracy, social acceptance and universal application. In these processes, verification and identification of human characteristics may be acquired from enrolment to subsequent use and re-use.

Emphasis is placed on robust storage and retrieval facilities necessary to gain social acceptance of the stages in the verification and identification procedures. They range from recognising the chosen sensor to representing the interface between the system and specific social circumstances. This is usually represented by an image acquisition system proceeding to a pre-processing storage to enhance input quality and exclude distractions in the environment, towards a process of normalisation. This is followed by feature extraction, in which, for fingerprint scanning, an image (arch, loop and whorl pattern) creates a template to discard biometric measurements other than those used in the comparison algorithm, so as to enhance the privacy of the individual and ensure that the file size is manageable.
It is arguable that social concern arises at this point in the process of implementation, when the template is stored. This commonly involves the use of a database or card storage facility so that a matching process analyses the template and subsequent input. This creates output towards a specified solution, namely access control management, in which social concern rests with the possibility that an individual may be exploited (BoozAllen, October 2009).

The second point of contention arises within the performance metrics for the system; ranging from risks of false acceptance or false match to false rejection or false non-match. Risks have also been identified from failure to enrol, failure to capture and exhaustion of template capacity, leading to the system having reached the maximum number of data sets capable of being stored. Risks of this nature led Rathur et al., (2001) to support the development of cancellable biometrics, akin to passwords or security tokens that may be replaced with subsequent versions. They proposed a process of cancellation by performing a distortion of the image before matching, so that the variation in distinction provides a cancellable strategy. This approach has been criticised however, as being prohibitively restrictive in its capability to apply only where multi-modal systems are used.

Lynch (2009) recognised that whilst controlling access to workplace environments poses challenges, technological innovation has helped to meet these challenges. He made specific reference to time and attendance, health and safety compliance and incident management, suggesting that in controlled environments, the use of biometric hardware ensures one hundred percent integrity. He suggested that this is true whether it is associated with iris or facial recognition, fingerprint or vein pattern recognition, with there being few differences in the benefit of each form.

Lynch (2009) placed more emphasis on the insurance of a robust and consistent solution, irrespective of form. In doing so, he pointed to the potential for this technology to save production costs and to guard against "buddy punching" (where workforce members may gain access to restricted environments using a third party colleague) with associated workplace implications. These included the potential to verify workplace
attendees in case of security alert or emergency evacuation. He also pointed to the increasing development of mobile solutions throughout construction sites in the United Kingdom and Ireland during the previous five years, providing for cross-site technology to be effectively used in the absence of telecommunications at each location.

In addition, Manning (2008) considered that access control and security are major concerns for United Kingdom enterprises. Security applications such as keys and swipe cards may be stolen or forged and key pads may be compromised when users rely on memory and integrity to secure access. The absence of any positive link between the system and user where physical and/or behavioural traits are measured represents another key compromise for security. Manning (2008) suggested that the implementation of biometric technology provides the only reliable means of identifying those with access authority, without the risk of theft or unauthorised sharing of identification.

From a practical perspective, biometric access control is ideally suited to the workplace environment (Manning, 2008) and provides simple processes to delete data when employees leave. Such systems are also flexible in providing practical applications for adding personnel on change of contract worker, access to consultants and visitors to the premises. The technology may also be designed to manage appropriate levels of access and, from a health and safety perspective, the existence of biometric-authorised individuals can assist in verifying evacuation procedures in emergency. It also has the capacity to comply with legal requirements for management to exercise a duty of care towards the health, safety and welfare of employees and other personnel via the Health and Safety at Work etc. Act 1974 (the Management of Health and Safety at Work Regulations 1999) and the Occupiers’ Liability Act 1957 (1984), in addition to the duty to maintain personal data in a secure way within the Data Protection Act 1998 and the Human Rights Act 1998, in which elements of privacy and integrity must be respected.

Despite the legal and practical benefits of access control, user acceptance is a critical issue in the current social environment, in which individuals identify with an increase in the surveillance society. In order for the technology to be viable, it must be easy to use
and avoid causing discomfort to its participants. It may be used to positive effect as a selling point when it is implemented in areas such as safety deposit and self storage facilities and in nurseries, educational establishments and care homes, where additional revenue may be gained when biometric systems are installed.

Wood (2008) suggested that if the objective of securing buildings is achieved and cost is kept to a minimum, biometric technology may be offered on a greater scale, largely in areas of law enforcement and public security. In addition, increasing environmental concerns relating to carbon footprints strengthen the value of biometric access control in providing building management in which lights and air conditioning systems may be managed in empty rooms, leading to energy efficiency benefits.

The Access Control Report 2008 (Wood, 2008) suggested that in the period 2008-2012, the growth of smart card and biometric technologies is likely to be the steepest with the United Kingdom demand for the integration of physical and logical access control by 2012. Balanced against cost-benefit analyses, however, rest a number of un-quantifiable variables that must be constantly acknowledged and managed. They included perceived risks of intrusion into private lives and associated potential for violation (Riley and Kleist, 2005). Effective communication and proper training may alleviate such concerns but their root cause must not be ignored. Perceptions of risk and integrity relating to implementation and performance in cases of disability, injury and religious objection, must be constantly considered and responded to. Riley and Kleist (2005) suggested that the business case should be qualitatively identified and documented, especially in the private sector, where, compulsion may not apply so that qualitative considerations can be balanced against quantitative edicts, in the decision making process.

Among the qualitative considerations, Riley and Kleist (2005) suggested that issues of increased convenience, enhanced service and more effective accountability should be considered. In cases of law enforcement, when compulsion or government edict apply acceptance cannot be a primary issue. In other cases, despite technology being inherently privacy neutral and socially indifferent Riley and Kleist (2005) suggested that in non-compulsory areas, social, legal and ethical implications should be
considered and organisations should be prepared to identify and address each issue as it arises.

The introduction of access control technology into the workplace has represented a change to both the working environment and perhaps working practices. Change of this nature can have a negative effect on performance and can detrimentally affect working relationships if it is not managed appropriately (Inalhan, 2009). Even when management considers the effect and consequences of change on the workforce, evidence has suggested that one-third of major change initiatives in the workplace fail because employees are suspicious of change (Inalhan, 2009). This may lead to major workplace difficulties resulting in reduced productivity and absenteeism, low morale, increase in errors at work, attempts to sabotage change and eventual loss of experienced personnel (Inalhan, 2009).

The key element in workplace change has stemmed from the emotional relationship a worker develops with the workplace. Inalhan (2009) suggested that people are linked to this environment through attachment, familiarity and identity, with any displacement breaking these emotional connections. The introduction of access control technology to a workforce previously unaffected by this may produce the same psychological effects and hamper its objective.

Inalhan (2009) adopted a Constructivist perspective in this article, enquiring into the meanings and understandings individuals and employees develop to make sense of how a change process of this kind will affect them. He used an Interpretive Phenomenological Analysis (IPA) to analyse the qualitative data collected from this study. This approach was adopted by Nicholson 1990 (cited in Inalhan, 2009) in his Transitional Cycle, in which he suggested that there are four phases, from loss of attachment to re-engagement with new attachments; beginning with:

1. An established working environment in which attachment is established (phase 1) followed by:
2. Loss of attachment leading to disruption and stress (phase 2);
3. A period of post-disruption and coping with loss (phase 3); leading to:
4. The creation of new attachments (phase 4).

This position may arise with the introduction of biometric technology for access control into environments previously unfamiliar with such technology and fearful of its implications. The Transition Cycle should be monitored and managed appropriately in order for individuals and employees to reach phase 4 in the model identified by Nicholson (1990). Management should recognise that employees experience a range of emotional stages from denial, anger, bargaining and acceptance in order to cope with change.

To productively respond to such employee experiences, Harrison et al., (2004, cited in Inalhan, 2009) suggested that a typical change management procedure goes through five phases, beginning with:

1. The information phase, where management outlines the nature of the change;
2. The inter-active phase, in which employees are engaged in the change;
3. A preparation phase, immediately prior to implementation, where the rationale and associated policies for change are articulated (this may be of particular significance when access control systems are imposed by government edict); followed by:
4. A familiarisation phase in which staff is encouraged to become accustomed to the new technology and its effects, and finally:
5. The after-care phase, in which problems are identified, monitored and responded to efficiently. This will be the phase in which any practical difficulties, for example, those associated with biometric enrolment will be identified and attempts made to rectify their effects to the satisfaction of individuals concerned. Sensitivity to the effect of change is vital at this stage where management should recognise that changes in individual perceptions of privacy and human rights may result in employee loss and grieving (Inalhan, 2009).
Workman (2009) agreed that an assessment of employee perceptions is vital in avoiding negative attitudes towards working practices that could lead to counter-productive behaviour ranging from absenteeism to a variety of retaliation responses. Workman (2009) concluded that data collected about the perceptions of information gathering for employment purposes versus that gathered for purposes of surveillance, revealed a benign view in the first instance, with the collection for employment mean at 4.6 (on a scale of 7) whereas that for the purpose of surveillance there was a mean of 3.2, indicating a less favourable social attitude towards the collection of data for surveillance purposes.

This led Workman (2009) to suggest that the strength of organisational management is vital in maintaining the psychological contract reflecting social belief about the reciprocal obligations between employers and employees. This kind of ethical and responsible attitude towards access control for securing the workplace has been based on perceptions of reciprocal benefit to the employer and employee relationship. Procedural justice appears to manifest from fairness and transparency in the consultation process, presenting an opportunity to raise grievances and engage in arbitration (Workman, 2009).

From a wider perspective, evidence suggested by Tangirala and Ramanujam (cited in Workman, 2009) suggested that if employees are not involved in consultation processes for strategies affecting them, they are more likely to find ways of retaliating against management, and, by definition, they are less likely to be committed to their work. In contrast, management provision of transparency and opportunities to engage, are more likely to lead to a greater level of commitment by employees, with an overall perception of job satisfaction and greater acceptance of organisational responsibility (Workman, 2009).

In assessing reasons for positive perceptions towards this technology, (Workman, 2009) applied the Theory of Planned Behaviour, to explain human behaviour modelled as a function of subjective norms, attitudes and perceived behaviour, concluding that the greater the perceived behavioural control the stronger the individual’s incentive to
perform the required behaviour. This research led to the conclusion that when end-users feel able to perform activity, such as compliance with security policies, and when they consider that compliance would be favourably received, they are more likely to accept and comply with the security policy. However, research also suggested that employees who had been employed for many years but had only recently been introduced to security policies, tended to carry out previous work practices in the absence of compliance, even when organisational influence demanded the contrary.

This was balanced however, by evidence that the effect of technical support towards employees previously unfamiliar with this technology enabled greater policy compliance by end users. This strategy has been further supported by Dror and Mnookin (2010) in their assessment that, if technology is going to be used to its maximum potential, the implications and the consequences of using it must be first understood, and any necessary adaptations must be made both to the technology and the way humans work with it.

2.8 Initial Legal and Ethical Perceptions

The link between law and ethics in implementing technology was brought into sharp focus in September 2007, when Michael Marper appealed through the United Kingdom courts and the European Court of Human Rights (ECHR) agreed to hear his case in objecting to the retention of his DNA information on a Home Office database, despite his never having been convicted of a crime.

In a judgement reported on December 4th 2008, the European Court of Human Rights ruled that Marper (then aged 45) and another applicant (S), a teenager, should not have had their fingerprints retained by the police. The data had been held by South Yorkshire police although neither was subsequently convicted of any offences. The 17 Senior Judges unanimously ruled that the keeping of information could not be regarded as necessary in a democratic society. In both cases the police had refused to destroy fingerprint and DNA samples taken whilst in custody but the ECHR ruled that the retention of DNA profiles resulted in discrimination and breached the individuals’ right to a private life.
The United Kingdom Government responded with a claim that retention of data from those not convicted could lead to their association with other crimes in the future, so the storage of DNA and biometric data in these cases was a proportionate response to tackling crime. In contrast to this however, the Scottish system differs to that of the United Kingdom, with the former destroying DNA samples taken from people not charged or subsequently acquitted following investigation.

In the House of Lords hearing, Lord Justice Sedley had defended his proposal to put the DNA of every United Kingdom citizen on the DNA database, in order to eradicate the imbalance of ethnic minorities on such systems. Sedley argued in favour of his proposal on the basis that civil liberties would be best adhered to if all United Kingdom citizens were treated equally and fairly by universal inclusion into the database. In this respect, Sedley’s reasoning paralleled the Code of Ethics observed by the International Biometric Industry Association (IBIA) relating to Safeguards for the Public; Respect for Competitive Technologies; Accountability in the Market Place and Free Trade.

In contrast, the Nuffield Council on Bioethics had condemned the retention of DNA on the National Database as unethical with the potential for presenting a Police State (Marks, 2007). Its Report entitled: The Forensic Use of DNA and Fingerprints: Ethical Issues, had argued for restricted storage of bi-information, applicable only to those convicted of crime (Marks, 2007).

In support of the Nuffield Council strategy, Kablenet (2007) cited the Liberal Democrat Shadow Home Secretary saying that the retention of DNA from thousands of innocent British citizens blurs the fundamental distinction between innocence and guilt upon which our whole criminal justice system depends. This has widespread potential impact in the United Kingdom with its police force having greater power than in any other country to sample such information, together with proportionally, the largest forensic database.

The Council urged ethical caution in linking matches between people and crime scenes, with Sir Bob Hepple QC, Chairman of the Nuffield Council on Bio-ethics, citing a
newspaper article having suggested that the British couple Kate and Gerry McCann, whose four year old daughter went missing in Portugal in May 2007, would have difficulty proving their innocence as a result of widespread reports of forensic links. And, critically, the Council reviewed the more recent generic use to which databases are being applied, for example, in the area of analytic “genetic predisposition to crime” with its potential for unethical implications.

Marks (2007) also alluded to a comment by the Nuffield Council on Bio-ethics in Gene Watch in 2006, in which it raised the profile of DNA insecurity when it revealed that a company used by the police to analyse DNA samples, had been covertly retaining samples and personal details of large numbers of people. But, whilst public confidence in ethical awareness may be damaged by revelations of this kind, the Nuffield Council responded to the Gene Watch issue with the suggestion that companies having custody of biological samples should be required to enter into a Material Transfer Agreement Standard (MTAS), applicable to all parties and subject to ethical review, so that common terms and conditions are established for the accessing of biometric samples.

A more specific strategy was announced in November 2009, that DNA samples regulated by the United Kingdom Government should be destroyed after six years in the case of children between 16-17 and in the case of adults arrested but not convicted of any offence. For serious offences however, where there has been conviction, caution or reprimand, the process of retaining samples indefinitely was supported, with children under the age of 16 having their data destroyed after 5 years following a first time conviction or minor offence but upon second conviction, caution or reprimand, their data may be retained indefinitely, on consistent terms to those of adults (House of Commons, Hansard, Ministerial Statements for 11th November, 2009).
2.9 Recognising Human Rights for Compliance

Turle (2007) argued that whilst security-based biometrics has an important role to play within commerce, organisations must recognise the data protection and human rights implications of the technology. Since 2007 all United Kingdom passports incorporate biometric data in an imbedded chip. February 2010 saw the introduction of a pilot system for the operation of full body scanning (subject to random passenger selection) at Heathrow and Birmingham Airports. A number of United Kingdom airports use iris scanning technology; whilst a number of European countries have established iris scanning technology for access control to buildings and membership to leisure facilities.

Turle (2007) warned of the risk of compatibility with individual rights to freedom and privacy, leading to a mix of legal and ethical considerations whereby biometric systems must comply with the European Convention on Human Rights 1998 and the Data Protection Act 1998. The former states that citizens are entitled to respect for private life and interference should only be permitted in specific circumstances. So a “private life” may operate both inside and outside the working environment and the latter regulates the processing of information identifying individuals. It requires that information (including biometrics) be fair and limited to specific purposes to which the individual has been notified at the time their personal data was made available.

Some more specific legal considerations apply to the possibility of biometric data being transferred across borders in the absence of consent, contravening the Data Protection Act 1998 (Principle 8) (Turle, 2007) and the risk of biometrics as physical or logical access control systems to workplaces and its potential for monitoring employees (UK Biometric Working Group, 2007).

The Working Group (2007) emphasised the legal requirement for consultation in this area whereas the German system established a consultation procedure based on Working Council approval for legal compliance. Whilst in the United Kingdom wider legal implications have been recognised in using biometric technology in the workplace, Howarth (2005) considered methods of collecting data and providing information on
how this information will be used, including informing employees of their access rights and rights to redress inaccurate data.

Howarth (2005) further suggested that security concerns should be allayed during enrolment in biometric schemes and during transmission over public networks. Still the most critical consideration appears to relate to the fear of identity theft so that citizens must be convinced that adequate security systems are in place to prevent theft of biometric data, given the widespread concern that once such data is stolen it may never be retrieved.

2.10 Privacy in Biometric Applications

Boulgouris et al., (2010) suggested that there is a dichotomy between the advantage of using biometric technology for security and the risk to personal privacy arising from the potential abuse of biometric information. This has formed the basis of academic debate, resulting in scepticism towards adopting biometric systems on a large scale. Boulgouris et al., (2010) suggested that a privacy protective and privacy sympathetic systems should be considered in the management of access control systems. The former should focus on protecting access to personal information via the application of trusted identities to manage risks of duplication, theft and misuse of data. The latter should focus on limiting access to personal data from unauthorised usage, via a strategy in which privacy concerns are at the forefront in the storage and transmission of biometric data.

In the case of access control Boulgouris et al., (2010) suggested that a fingerprint system is less likely to be used with ease for covert purposes than a facial recognition system, with capability and risk being addressed in equal measure. From the perspective of “best practice”, Boulgouris et al., (2010) suggested that four main issues are paramount in the design and usage of systems of this nature. They begin with considerations of system scope and capability, and proceed to consider the effects on managing data protection, establishing effective control of personal data by system users and ensuring the disclosure, auditing and general accountability of the biometric system.
2.11 Application of Privacy in Multi-Modal Systems

This research considered multi-modal systems based on fingerprint analysis and facial recognition for access control. It recognised that, whilst there are a number of advantages in using this type of system, the associated disadvantages must also be alluded to. From a positive perspective, multi-modal systems increase population coverage by providing for alternative traits to be considered in cases of injury or illness. This leads to deterrence against successful spoofing and evidence suggests (Boulgouris et al., 2010) that the reliability of systems improves when unconnected traits are used: for example, an eye used with a fingerprint or when right and left eyes are used together.

Against this perceived advantage, there are recognised drawbacks in using multi-modal applications; resting primarily with the higher cost associated with setting up systems for multi-modal recognition. There are also risks of social perception of a more invasive process and inconvenience, with privacy concerns being at the heart of social scepticism, based on a perception that multi-modal applications retain proportionally larger samples of biometric trait.

The emphasis of this research rests with privacy issues and Boulgouris et al., (2010) have suggested a number of guidelines to achieve greater social acceptance of multi-modal applications. There are suggestions that templates should be randomised to avoid risks of data leakage, to the proposition that the number of biometric traits should be associated with the perceived risk. There are also suggestions that multi-modal systems should be modular with templates being privacy compliant so as to minimise the risk of cross-reference to other databases holding the same information.

Suggestions have also arisen towards using a multi-modal enrolment model in which two different biometric readings are collected. This would use facial recognition and a fingerprint or fingerprint recognition from two different fingers, with samples processed using “feature extraction technology.” This could consider for example, the positioning of eyes to nose in facial recognition and points of ridges and patterns of prints in
fingerprint scanning systems. This strategy would result in a set of features being produced depending on the biometric trait, capable of transfer to a binary string, resulting in the production of a distinct binary template.

Boulgouris et al., (2010) suggested that the creation of the type of template discussed above may be subsequently associated with a specific “standard” (similar to the ANSINCITS 378-204 standard) (American National Standard for Information Technology X Finger Minutiae Format for Data Interchange). This could be used for authentication and privacy purposes, with verification arising from the production of biometric traits requested at enrolment. Separate identification would be arrived at by the subject being requested to provide the same biometric traits s/he produced at enrolment, resulting in the generation of two new binary templates represented as 1:1 and 1:2 (Boulgouris et al., 2010).

2.12 Application of Standards and Academic Projects

A series of security Standards and funded projects have been introduced in recent years to supplement the social, legal and ethical regulation of biometrics.


In 2008 the ISO/IEC TR 24714-1: 2008: E Standard entitled Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies was established. It sought to clarify societal, cultural and ethical issues relating to the use of biotechnologies for identifying people. This document relates to the design and implementation of biometric technologies associated with legal and societal constraints and the assurance of accessibility for the population as a whole. This provides guidelines for the stages in the life cycle of a system’s biometric elements. It spans (but is not confined to) legal frameworks for the capture and design, implementation (enrolment and usage), inter-operability of data storage and security, updates and maintenance, awareness and training, evaluation and audit. This Standard was followed
by a number of European Engineering and Physical Science Research Council (EPSRC) funded projects, ranging from EnCore (ensuring consent and revocation); PV Nets (Privacy and Value Networks); VOME (Visualisation of Other Methods of Protection) and RISE (An international platform devoted to Ethics of Biometrics and Security Issues: (2914/2009: riseproject.eu).

The ISO/IEC Report 2008 focused on societal, cultural and ethical issues relating to the use of biometrics in security systems for identifying people. This Standard recognises the diverse application of biometric technology in public and private sector applications to authenticate identity, secure national borders and manage access to secure sites, including buildings and computer networks. It provides guidance on the design of systems to capture, process and record biometric information.

The Report was delivered by Fernando Podio (Chairman of the ISO/IEC Joint Technical Committee, IT Sub-committee, and 37Biometrics). Podio recognised that: “For decades biometric technologies were primarily used in law enforcement applications,” (Preston, 2009, email: 17th February).

Podio (2009) suggested that the increasing use of biometrics for multiple applications provides opportunities for the development of enhanced security for physical and logical access control. He further suggested that ISO/IEC: TR 24714-1: 2008, provides practical assistance to a range of personnel from manufacturers, suppliers, managers and users of biometric systems to enhance cross-jurisdictional and societal compliance for implementing biometric technology into commercial applications.

The 2008 Report supporting the Standard focuses on the provision of guidelines for ensuring privacy and protection of personal information, health and safety, access control for workplace management and usability, together with policies to promote social, cultural and ethical acceptance of biometric systems. Whilst it does not address specific government policy, the Standard supports the appropriate capture and design of initial client requirements and legal compliance for deployment, enrolment, usage and inter-relationship with other systems.
From a practical perspective, the Standard provides guidelines for maintaining and updating associated data; providing awareness of training requirements, in house evaluation of systems and system audit. Primary stakeholders, from designers, implementers and system operators, may use the recommendations in the Standard to establish, enhance and maintain acceptance by improving public perception of well designed systems. This may facilitate the efficient introduction and operation of systems, whilst enhancing long-term cost reduction and increasing awareness of the range of accessibility requirements working towards enhanced privacy to comply with legislation regulating Human Rights, Data protection and the Regulation of Investigatory Powers.

The 2008 Report (ISO/IEC, 2008: 42.2 Privacy, P. 4) recognised that biometric technology may be considered a component of Privacy Enhancing Technologies (PETS) to protect privacy by eliminating or reducing personal data, preventing unauthorised, unnecessary or undesirable processing of personal data without losing system functionality. The Standard recognises the right to privacy established within Article 17 of the International Covenant on Civil and Political Rights that: “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation,” (Office of the High Commissioner for Human Rights).

In addition, Privacy Enhancing Technologies (PETS) suggest a number of generally accepted rules to protect privacy, considering that as little personal data as possible be stored. It also contends that data necessary for storage should be kept in an encrypted way. Raw data should be destroyed as soon as possible and it should be monitored in an anonymous way, whenever this is possible. It further provides that the use of central databases should be avoided, with priority given to individual subjects’ control over their personal data. These measures are enhanced with the use of consistent evaluation tools and certificates of verification, presenting a guarantee of an appropriate level of trust and confidence in the system.
With the long-term use of biometric systems, the Standard discussed above, recognises that a number of additional issues may emerge for management consideration, arising from changes in methods of providing informed consent. This may arise from individuals migrating to an age of majority, the change of mental capacity and the death of a subject, to the need for the system to notify data subjects of any changes in using the system. This leads to the implementation of principles for biometric systems ranging from assurance of transparency for the practical use of data; consent in collection, use, disclosure and retention of data by data subjects. It extends to preference for opt-in facilities to acknowledge system use, policies for limitation of purpose, collection and treatment of data and statements of adherence to performance criteria, in which systems will function in accordance with specifications, to access rights for data subjects and protection of privacy.

From a legal perspective, three-factor authentication may be the preferred security solution but two-factors are sufficient for most commercial applications. Legal challenges may be based on the reliability of the biometric system, so aspects of performance and overall security in the total system (ISO/IEC 27002:2005) will be the most significant aspect to emerge from a case. Liability may arise from the failure to protect and service biometric systems so these issues and their consequences must be considered by manufacturers, suppliers and management.

Exclusion of liability for system malfunction is usually not permitted or desirable within the terms and conditions of business, with the subject being unable to affect or control technical aspects in the manufacturing, supply or management domain. Provision should be made for alternative methods of identification and verification where individuals may otherwise be discriminated against by disfigured or missing fingers, facial scars and an inability to present biometric identification, due to disability of other discriminating factors.

In the workplace management of physical or logical access control, employee rights should be a paramount consideration. This may be ensured by management involvement of trade union representatives and equivalent strategies for appropriate management of
biometric systems. The German Government has made specific provision for workers rights to be protected with the compulsory participation of Works Councils.

Biometric systems should be accessible to all and should not disadvantage any subject. Usability must be considered within both physical and logical environments and alternative systems must be available as a contingency. The 2008 Standard recognises “accessible” systems as having universal characteristics for equality of use, flexibility, simplicity, ease of understanding, clarity and ease of tolerance in cases of system error. The system should be capable of use with minimal physical effort, representing ease of approach and use via a range of tactile audio and visual prompts in its user interface.

Many countries have developed inclusive policies for implementation, supported with legislation. In the United States, the Americans with Disabilities Act 1990 (Public Law 101-136 of the 101st Congress, enacted July 26th, 1990) and the European Standards and Workshop Agreements (ISO/IEC Guide 71, Guidelines for Standards) developed to address the needs of older people and those with disabilities. The United Nations Standard Rules on Equal Opportunities for Persons and Disabilities (1993) made special provision for people with disabilities in education, employment, social security, culture, recreation, transport and accessibility to the built environment and information, whilst the domestic standard (JIS X8341) was established in May 2004 to protect the accessibility of biometrics in Japan.

From a health and safety perspective, subjects must be informed of any risks that may arise from the use of biometric systems and individual concerns must be responded to. Direct medical implications of using this technology must be considered where physical contact with a device may result in infection and illumination by visible or invisible light may result in damage to sensitive organs. Indirect medical implications must also be practically responded to, where there may be perceived privacy concerns relating to subsequent insurance policies or employment status, arising from the accessibility and / or sharing of biometric information between organisations. Practical responses should be made to eliminate negative perceptions with organisations referring to and complying with health and safety legislation.
The usability of this technology to comply with optimal performance should be considered in the context of climate, in which environmental conditions may present problems for the efficient working of biometric systems. There must be prevention of contamination and cross-contamination arising from devices located in engineering or industrial locations or areas of specific sensitivity. Organisations must recognise that biometric devices located in external areas may be subject to vandalism and high noise levels that may compromise the efficient working or reliability of this technology, with associated risks presented for the reliable collection and verification of data.

From social and ethical perspectives, in addition to a base-level agreed Good Practice Policy, ISO/IEC TR 24171-4, 2008 suggests that diversity must be recognised and respected, where cultural groups may raise objections to touching shared surfaces such as fingerprint scanners. In time and attendance systems, appropriate imagery should be applied to devices to ensure full cultural awareness of system requirements. Anonymity may be a primary concern in some cultural environments and the system may respond with a need only to verify entitlement to access or to prevent multiple environments, rather than requiring personal details from each subject. Facial recognition systems may not be socially acceptable in cases where the normative behaviour of an individual is to wear a veil, headscarf or full burkha. Similarly a system that is negatively influenced by bodily embellishments represented by jewellery, tattoos, clothing or facial hair may represent an unacceptable system of identification in modern culture.

Manufacturer, supplier and management awareness of social, legal and ethical aspects of biometrics are prerequisite at every phase of biometric implementation for access control and subsequent management. Stakeholders should strive for the optimum acceptance to be achieved for biometric applications to be of greatest tangible benefit to society. This supports the Utilitarian philosophy that the willingness to use this technology and its overall acceptance will be detrimentally affected if the user does not recognise its benefit.

The 2008 Standard recommends success factors to support the procedures previously discussed. They may be achieved when the individual recognises the biometric system
as representing an advantage to the security tasks that they must carry out supported by a high level of performance. This may work towards establishing a general perception of trust and safety in an environment in which biometric data is maintained securely and not used for peripheral purposes.

Positive attitudes to biometric systems correlate with simplicity and speed of use, convenience and perhaps a positive attitude towards the technology by more frequent exposure to biometric systems reported in the media. Suggested actions for acceptance testing of biometric systems from the 2008 Standard include the piloting of biometric applications and conclusions drawn from all groups: from age, gender, education, occupation, expertise, culture, ethnicity, role within society and attitude to authority. There should be audit trails of the user population, to establish the concerns of respective subjects and contingencies for additional testing and re-designing of systems through a process of development. Organisations should have policies for re-enrolment with age and there should be investment in developing systems to reduce the rate of false rejection with its potential to result in loss of security. Correlations between false acceptance and false rejection should be included in dialogue with subjects with the provision of information and guidelines appropriate to both technical and non-technical people, available in languages to serve the diversity of subjects. Management should ensure that subjects are sufficiently familiar with biometric systems and their application before engaging in acceptance testing, with informed knowledge representing an important factor in securing subject acceptance. A policy of providing constructive information should be included in the education and marketing processes used to introduce biometric systems into public environments.

In this respect, Stephenson (2007) suggested that adjustability should be consistently rolled out in response to false acceptance and rejection rates, where usability requirements have traditionally relied on low rejection rates often leading to an unacceptably high false acceptance rate. Stephenson (2007) suggested that the value of adjustability rests in its capability to lend individualism to biometric access control systems to suit the environments in which they are used. Where robust authentication is necessary, Stephenson (2007) suggested that secure access control or strong
authentication service (SAS) should combine a biometric system such as fingerprint scanning or facial recognition with PIN or smart card authentication. He suggests that this will enhance user perception of security and reliability where door access uses SAS, while computers use only fingerprint scanners integrating with the existing authentication infrastructure to fulfil basic functionality requirements.

In addition to the suggested strategies of Stephenson (2007) and the 2008 Standard, a series of projects have been developed in this area since 2009, funded by the European Commission. The British Computer Society (BCS) published a Best Practice Code for the use of Biometrics in August 2009, whilst the Engineering and Physical Sciences Research Council (EPSRC) has funded a series of projects including EnCore (Ensuring Consent and Revocation). This has assisted consent for sharing personal data and revocation by developing an understanding of the meaning of consent and revocation in industry, government and commerce. This strategy is being implemented through a 5 year project undertaken by the London School of Economics, Warwick University and the Universities of Leeds and Oxford.

2.12.2 The British Security Industry Association (BSI)

This is the trade association for the professional security industry in the United Kingdom. In 2009 the Association undertook research into the benefits available from access control technology within the United Kingdom. Referring to this research, Sussman (2009: 1) said:

"There are many benefits of using an access control system. Increased security and point of entry to sites, buildings and rooms are obvious ones but there is also visitor monitoring, automatic number plate recognition, integrated security and bottom line through operational efficiencies that makes the technology worthwhile."

The BSIA Access Control Centre has produced a number of guides on the benefits of using access control technology in working environments from office spaces, schools and manufacturing sites. The continued terrorist threat has heightened public sector awareness of the need to control access to their premises. This is combined with the
increased awareness of legal obligations to discharge duties of care to pupils and students, employees, contractors and visitors to premises.

Smith (2007) suggested that access control to protect premises and information is just one of a series of factors impacting on owners and managers of premises. Smith (2007) pointed to the legal duty of care imposed on stakeholders to ensure the safety of those who use premises, regulated by the Occupiers’ Liability Acts 1957 and 1984 and the Health and Safety at Work Act 1974, combined with the Management of Health and Safety at Work Regulations 1999. He pointed to the more established systems in which access control has been managed at reception areas, using recording and logging facilities in which entrants are provided with badges to authorise entry. Whilst entry may be monitored securely using this method, Smith (2007) argued that egress cannot, leading to security risks in identifying those who are in the building at any given time.

This uncertainty in security system has been responded to within a number of organisations, using biometric identification to apply fingerprint scanning and facial recognition technology, among other applications. These systems regulate access and egress by comparing unique human characteristics, usually employed where higher levels of security are necessary or desired but Smith (2007) stressed that biometric systems should not be regarded as a panacea in all cases. It is likely however, that with advances in technology combined with improvements in reliability, affordability and operational speed, this technology will become used in more diverse ways in the future; leading to the wide-scale provision of higher security at reasonable cost being available to public and private sector, industry and education.
2.12.3 EnCore (Ensuring Consent and Privacy)

This is a collaborative project investigating informational privacy by representatives of United Kingdom industry and academia. The broad aim of the project is to adopt cost effective consent and revocation methods to control the use, storage, location and sharing of personal data. This provides a mechanism by which individuals may control the use of personal information held in the public domain and help to foster individual confidence in participating in the digital age, towards the benefit of the wider society.

The EnCore project participants include public organisations and institutions of education from Hewlett-Packard Laboratories, HW Communications Ltd, London School of Economic and Political Science, Qinetiq, the Ethox Centre at the University of Oxford and Digital Laboratories at the University of Warwick. One of the project deliverables refers to reports being established on techniques, management strategies and best practices for business; involving prototypes, legal recommendations and proposals for certification and validation.

The project is case study driven, based on investigating current practice, requirements for and barriers to improvement and social, legal and ethical considerations towards representing consent and revocation requirements for business. The methodology produces broad outcomes from dissemination of knowledge gained towards developing a regime based on academic policy, legal regulation, standards and best practices. The proposed outcome of this project is to make giving consent to the use, storage and sharing of personal information as rigorous, reliable and easy as turning on a tap and revoking that consent as rigorous, reliable and easy as turning it off again.

2.12.4 PV Nets (Privacy Value Networks) (2008-2011)

This project is being undertaken by the University of Oxford from September 2008-August 2011 in conjunction with Human Computer Interactions. It has challenged the government suggestion that the public is generally unconcerned about privacy, by examining the cost and benefit of collecting and storing data about individuals and the value of holding information for specific purposes. Whilst identity and privacy have
been major concerns over recent years, the government has justified the identification of citizens and tracking of social behaviour for security reasons. Commerce also argues that the need to track customers' identity is based on modern customer expectation that personalised services will be delivered through targeting information and identifying conventional business opportunities.

Public polls conducted by government have perceived the general public as being unconcerned about privacy. It argues that citizens support identification and surveillance and commerce argues that customers are content to pass on personal information for returns relating to discounts and entry to prize draws. But once citizens experience negative consequences, they are more likely to respond by rejecting automated services. They may respond by refusing to register information or by providing false details, leading to the risk of economic damage and the collection of data with no practical value.

This project focuses on the lack of clarity between stakeholders as to the definition of privacy and its meaning in everyday society. Whilst past studies have undertaken sporadic surveys, the PV Nets project is based on an examination of stakeholder perceptions of privacy over time. This facilitates practical responses to experiences of positive and negative effect of personal data collection, retention and sharing processes. The PV Nets project is based on the philosophy that in order to collect quality empirical data on individual perceptions of privacy, it is necessary for the individual to reveal things they would prefer to keep private. The contention of the PV Nets project is that methodologies can be developed and utilised to break the privacy paradox.

Brown (2010) in an article entitled: “Quantifying people’s trade-offs across liberty, privacy and security”, referred to a study undertaken by RAND Europe in 2009. RAND is an independent think-tank serving the public interest by improving policy-making and finding public-private solutions to shared problems. The RAND study reported on the results of a discrete choice modelling strategy aiming to objectively understand practical privacy, liberty and security trade-offs undertaken by individuals, to best prepare policy-makers’ understanding of individual preferences in this area. The study used
three practical cases: applying for a passport; travel on the national rail network and attendance at a major public event such as the opening ceremony of the British Olympics in 2012. A panel representing a weighting towards United Kingdom internet users, was compiled and asked to choose between different alternatives for each of the stated cases.

Analysis of the outcomes from this data revealed that individuals were prepared to pay for the installation of CCTV cameras with facial recognition systems. They were also prepared to be exposed to body scanning technology and x-ray machines, to enhance security measures in the areas identified by the case scenarios.

2.12.5 VOME (Visualisation of Other Methods of Expression) (2008-2012)

This study is being undertaken at the Royal Holloway University, London between October 2008 and March 2012, investigating a multi-disciplinary and innovative approach to achieving assured privacy and informed consent, by engaging stakeholders about privacy, consent and identity management.

VOME focuses on how user communities engage with information privacy and consent in on-line interaction. The project aims to develop conceptual methods of on-line privacy to facilitate clearer on-line privacy disclosure choices for users. The important link between VOME and access control measures rests with its ultimate capability to develop better dialogue between the designers of privacy and consent functionality and their users, based on the premise that there is a gap between those who design and deploy electronic processes and those who use them.
2.12.6 RISE (Rising pan-European and International Awareness on Biometrics and Security Ethics)

RISE is being funded by the European Commission involving 9 European and non-European partners in 8 countries (5 European Member States and the United States, China and India). It has three university partners, two private research centres, two stakeholder associations in addition to a public research institution and a consultancy, furthering the work of two previous projects in this area: BITE and HIDE in 2005.

The current project focuses on differences between the approaches of the European Union and India (with their diversity of ethnicity, social and religious culture) on policy issues relating to security, data protection and privacy. The aim is to promote international dialogue between the two states on these topics. In line with the growth of the Indian commercial market, concerns have arisen in areas of security and personal data. This has led to Western pressure for Indian organisations to introduce regulations according to European Union and United States standards to safeguard privacy and promote confidence in foreign investors.

The Indian Government has responded by initiating a policy of providing each citizen with a biometric national identification card (the UID Project). The Head of this project, Nandan Nilekani has commented however that:

"...biometric identity cards will provide an identity also to the millions of people that do not possess any proof of existence ....and it will help fighting terrorism and criminality. But the huge on-line database that will retain citizens’ personal information may itself represent a threat to privacy and data protection." (Emphasis added) (India, 14s, 2009: info-4security.com)

The mission of RISE is to create an internationally recognised framework for the planning and managing of security policies relating primarily to biometrics. It will consider the ethical implications of biometric identification technologies focusing on respect for the integrity and dignity of body and the protection of the privacy rights of vulnerable communities.
2.13 Social Implications of Implementing this Technology

Biometric systems have become the technological centrepieces of national and supranational policies (Petermann, 2006). While this technology has traditionally focused on providing solutions for terrorism, crime and ensuring appropriate identification (Organisation for Economic Co-operation and Development, OECD, 2004) (Petermann, 2006) social acceptance is only likely to be achieved when citizens are assured that their rights and liberties will continue to be respected and the integrity of their data guaranteed.

Threats to establishing social acceptance are evident, due to the relatively tight schedule for introducing and implementing the technology into society. This is coupled with the need for constant refinement, to achieve social perfection and to clarify uncertainty associated with the cost of implementation. These pitfalls, coupled with the absence of clearly justified, objective communication to citizens, continue to hamper the consistent progress of social acceptance.

In 1999 the US Army commissioned a report from the RAND Institute, relating to the legal, ethical and sociological issues raised by biometric technology. This led to the identification of three specific areas of concern, including risks of function creep, perceptions of tracking and association with data misuse (Mordini and Petrini, 2007). Following the RAND Report, biometric privacy issues were investigated in 2003 by the European Commission Advisory Body on Data Protection and Privacy, leading to the publication of a Working Report. The Report emphasised the need for biometric technology to be clearly aligned with explicit and legitimate purposes. It also raised concerns about incompatible re-use and the application of biometric access control systems obtained from physical traces unknowingly left by individuals. The Report recommended that biometric technology should be implemented to enhance personal privacy, whilst reducing the need to process traditional personal data relating to name, address and other aspects of hard identification.

The question of social perception from the experience of using biometric systems was further raised by in the Organisation for Economic Co-operation and Development
(OECD) in a report published in 2004. The report was based on guidelines it had produced in 1980, suggesting that there are two main policy points influencing the national debate on biometric application. Firstly, it is generally unacceptable to store biometric data in a central location or database and secondly, the recognition that biometric data is sensitive and subject to legal controls (cited in this article from the Ontario Privacy Act 2007 and the New Jersey Biometric Privacy Act 2007).

Following the social, legal and ethical issues considered above, a report was published in 2005 by the Institute for Prospective Technological Studies, highlighting five areas of potential public concern. They arose from risks of invasion of privacy, where a biometric template may prevent people from changing identity, even in cases of social need associated with witness protection programmes. This report also pointed to social and economic issues and the practical need to cater for natural differences arising from the ageing process, effects of disease, disability and risks associated with identity errors. It also considered legal aspects of transparency and privacy in compliance with data protection and human rights legislation.

Petermann et al., (2006) suggested that the protection of personal data will continue to detrimentally affect the achievement of coherent social acceptance of biometric technology for the foreseeable future. He (Petermann et al., 2006) also suggested that the importance of social and political discourse in this field should not be underestimated, where concerns linked to the technology are expressed with the public in practical contexts.

Petermann et al., (2006) considered that fingerprint authentication may be temporarily compromised by injury, with the risk of permanent loss arising from scarring or intensive manual work, leading to destruction of the fingerprint template. In contrast, whilst the record-ability of facial recognition may be compromised through injury or deformity, in the case of localised damage, the face as a complete feature, remains recordable, and this may lead to more general social acceptance of this technology in terms of reliability and accuracy. But, the practice of the UK Border Agency, in prioritising the use of fingerprint and facial recognition for identification, arguably risks
negative social responses based on perceptions of narrowing the choice of available systems.

Irrespective of the chosen technology, social acceptance will only be secured when there is general perception of consistent government processes to protect the privacy of the individual. There have been a variety of responses to the universal concept of "harm" and the role it plays in organisational control. Nelson, (2004) argued that the public policy debate for balancing technology is informed in the name of preventing harm, with the terrorism threat to liberty and the right of privacy. Political authority is viewed as both a threat to and a panacea for social liberty and privacy of the individual.

In this respect, Mill (1956:4) interpreted the concept of "harm" by justifying the extraction of liberty in a social context, on the basis that:

"The sole end for which mankind is warranted individually or collectively in interfering with the liberty of action of any of their member, is self protection. That the only purpose for which power can be rightfully exercised over any member of a civilised community against his will is to prevent harm to others."

This perception of establishing social confidence in the control mechanisms operated by government is particularly important post September 2001 society, where regulations enabling the gathering and sharing of information and the polarising of power by the government and intelligence has been increasingly evident in the name of addressing the "war on terrorism" (Nelson, 2004:261). This has arguably led to a society in which there is social perception of political authority taking precedence over civil liberties, with detrimental implications for the assurance of democratic principles.

In some respects, however, the concept of privacy has not been compromised by the technology. Where facial recognition systems are used in public areas, there is an argument that privacy is not delimited because citizens cannot expect privacy in guarding their facial features in the public domain. In the case of United States v Dionisio (410U.S. 1[1973] (Nelson, 2004:262) in which it was noted that:
“no person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world, ” (Cohen, cited in Nelson, 2004: 265).

Indeed Katsh (cited in Nelson, 2004) suggested that social acceptance may be less compromised by the implementation of this technology than by the control the citizen may have over their personal data. And Mill (Nelson, 2004) recognised that legislative provisions may strengthen ways in which surveillance is carried out and information is gathered in order to foster a balance between access control and consent. In this respect, privacy may be considered as a component of personhood (Nelson, 2004) where there must be justification for government invasion or that of business entities and private individuals.

On the question of gaining and maintaining social acceptance, Clarke (1998) argued that if the foundation of society is of social significance, social impact assessments should be conducted to objectively consider the impact of biometric technology on people. Clarke (1998) suggested that data surveillance technologies in general and biometrics in particular, should be subject to impact assessments following a set criteria from: full public disclosure of the technologies, publication of results and consultation opportunities from active public participation in design and agreed controls, to balance social, legal and ethical interests.

In contrast, a report published in The New York Times (December 12th, 2001) revealed the results of a survey conducted on the political landscape after the terrorist event of September 11th. It revealed that 65% of respondents said they would not support government monitoring of ordinary American citizens, whilst 48% supported wiretapping by government to deter terrorism and 44% objected to this practise on grounds of civil liberties (Nelson, 2004). And a Harris Poll conducted in October 2001 (Harris Interactive 2001 in Nelson, 2004: 268) revealed that Americans called for a balance between the introduction of new surveillance technologies to combat terrorism and an assurance that law enforcement applications of technology would not extend beyond its stated purpose. This led to the conclusion that:
"In order to foster social acceptance, government must balance political authority to protect individuals’ privacy with careful strategies to avoid adverse public perception."

Bali (2009) suggested that research of this kind on public opinion has consistently shown that frames or patterns of selection, emphasis and exclusion furnishing a coherent interpretation and evaluation of events can influence social thought and support for issues under investigation. This has led to general agreement that “how citizens think about a public issue, depends on how it is framed.” (Sniderman and Theriault, cited in Bali, 2009; Gamson and Modigliani, cited in Bali, 2009).

Using what they referred to as one-sided frames to induce positive or negative shifts in attitude depending on the issue being highlighted, (Bali, 2009) showed that participants exposed to edited news coverage of the Ku Klux Klan in which the event highlighted the issue of free speech (supportive frame), revealed higher levels of social tolerance to the Klan than those exposed to corporate video in which concerns were raised about the disruptive effects on public order, (opposing frame). This suggested that gaining public opinion using the framing process may determine the level of acceptance or rejection of, in this instance, social attitudes towards the implementation of biometric technology.

In order to ensure that results are objective and reliable therefore, Hague (2002) suggested that care must be taken in the design and implementation of empirical investigation, to ensure that there is a balance between questions about public governance and the democratic principle of citizenship. Framing issues related to anti-terrorist laws and institutions, focusing on internal and external security must be balanced with social issues relating to privacy, freedom of expression, political dissent and equality, relating to social entitlement (Hague, 2002).

In response, August 2006 saw the launch of the National Science and Technology Council Reports entitled: “Privacy and Biometrics: Building a Conceptual Foundation” and the “National Biometrics Challenge Report.” But despite universal acknowledgement of social, legal and ethical impacts on society, Mordini and Petrini (2007) argued that the overriding concern should be for human dignity following the
principles of the Magna Carta and those of the European Charter of Fundamental Rights.

Mordini and Petrini (2007) suggested that such basic human principles should be primarily acknowledged in a developing environment in which body parts are increasingly captured and stored in central databases. They are increasingly traded as commodities by both commerce and government bodies, in an environment in which they may be used to enable powerful organisations to exercise social control over individuals (Clarke, 2001).

In areas of social exposure, there is a long history of using biometric technology in casinos and associated with access control to commercial enterprise, such as Walt Disney World. On a larger scale however, the events of September 11th led to a reigning-in of commercial applications via major government initiatives (Gibson, 2009). Beyond social implications, Riley et al., (2009:14) highlighted the importance of considering cultural aspects in researching the social acceptance of biometrics, in their paper entitled: “Culture and biometrics: regional differences in the perception of biometric authentication technologies.” They focused on how people perceive biometrics from one culture to another and how concerns can affect the successful implementation of such systems.

Riley (2009) pointed to the importance of understanding cultural perceptions in their assessment that biometric technology will eventually be used in almost every transaction requiring authentication of identity. Whilst individual concerns relating to data security and function creep have been readily documented, Riley et al., (2009) suggested that there have been fewer surveys conducted into the underlying question of how potential users of biometric systems perceive the technology. They point to research conducted by Deane at al., (cited in Riley et al., 2009) in which 76 people were surveyed about their attitudes towards biometrics, concluding that biometric technology was rated less acceptable than passwords at that time.
But in a more recent survey conducted in 2004 (Biosec, cited in Riley et al., 2009) involving 204 participants from Finland, Germany and Spain, results suggested that the majority of participants were positive about the use of biometrics in air travel, despite having concerns about the use of the technology for this purpose. In areas of personal health and hygiene about 50% of those surveyed expressed concerns about potential loss of privacy with evidence of cross-cultural differences between Finland, Germany and Spain, with German participants revealing the greatest knowledge and most positive attitude towards biometric use.

Subsequent laboratory based usability evaluation conducted by Toledano et al., (cited in Riley et al., 2009) revealed parallels between individual privacy concerns and confidence in the technology. Whilst research was conducted by the United Kingdom Passport Service in 2005, testing over 10,000 participants in multiple United Kingdom locations suggesting that most people were in favour of using some form of biometric technology in conjunction with national passports (United Kingdom Protection Services, 2005 cited in Riley et al., 2009).

In his assessment of national culture in the context of biometric acceptance, Hofstede, (cited in Riley et al., 2009) suggested that there are five constructs forming national culture. He pointed to power distance: in which a society as a whole accepts unequal power distribution among its members, with people at the low end of the power hierarchy as likely to accept power distance unequally as those at the top; with Al-Gohtani, 2002; Everdingen and Waarts, (cited in Riley et al., 2009) suggesting that high power distance scores correlate with negative impact on technology acceptance across countries:

*Individualism:* equating to the relative importance of individuals within society compared with collectivist societies, where greater importance is placed on the family;
Masculinity: different between male and female gender roles with masculine societies tending to have more assertive and competitive values compared with feminine society

Uncertainty avoidance: at high level, equating with individuals being less comfortable in novel or less structured situations; and

Long term orientation: cultures in this category having more respect for tradition being oriented towards long-term future rewards as opposed to short-term benefits.

In testing his model, Hofstede’s cultural dimensions were applied to India, South Africa and the United Kingdom. India was associated with an emerging economy and market for biometrics; South Africa, although culturally and geographically different to India, was associated as emerging as a proponent of biometrics to regulate violent activity and the United Kingdom was included as an example of a developed country.

Hofstede considered the application of the technology acceptance model (TAMs), with primarily, the original model suggested by Davis, (cited in Riley et al., 2009) to investigate how systems are perceived. He contended that a technology acceptance model approach was not suitable in his evaluation because this model uses a defined approach of previously accepted dimensions. This is poorly suited to exploratory investigation and largely associated with assessing systems that people may choose, rather than have imposed upon them by government or commercial interaction.

Hofstede used an on-line survey administration methodology to distribute to India, South Africa and the United Kingdom, with Indian and South African respondents rewarded for completing surveys whilst the United Kingdom followed a snowball approach, without reward. The results of the survey revealed clearly defined cross-cultural differences, with Indian respondents displaying the most positive attitude towards biometrics and the United Kingdom respondents, the least, despite India being a collectivist country and the United Kingdom having an individualist approach.
Hofstede noted that power distance scores were positively associated with willingness to use biometrics and literature revealed that this technology would be perceived more positively in individualist societies. Whilst masculinity, was traditionally thought to be negatively associated with technology, the survey revealed positive perceptions, whilst the construct of uncertainty avoidance did not display any clear relationship with biometrics in the empirical study. This suggested that Hofstede’s cultural dimensions cannot be relied on to explain cross-cultural differences in perceptions of biometric technology.

Riley et al., (2009) attempted an explanation of the results of this survey as compared with the theoretical cultural dimensions. This suggested that local, contextual characteristics specific to India, South Africa and the United Kingdom, more effectively explain the results of the empirical investigation with United Kingdom participants likely to have been influenced by the (then) government proposed Identification (ID) Card scheme.

Whilst South Africa’s experience of violent crime may explain individual fears for personal safety and authentication, Indian respondents showed most favour to biometric technology (despite theoretical perspectives suggesting that India may have the greatest reservations about biometric technology). But empirical evidence revealed most favour from the Indian category, perhaps explained by the relatively strong position of Information Technology in Indian society as compared with the other countries surveyed. This suggested that as society becomes more knowledgeable about and familiar with this technology, it is less likely to display reservations as to its value and implementation.

The two strongest correlations between theory and practical investigation remain in areas of data security and personal safety but Riley et al., (2009) alluded to the relative limitations in this research, with investigations having been conducted wholly in English. This may have hampered meaningful comparison, whilst the issue of reward may have affected drop-out rates for on-line surveys. In other respects from the nature
of participant responses and respondent demographics, little difference is evident (Fricket et al., 1999 and Roberts et al., (cited in Riley et al., 2009).

Whilst inconsistencies emerge between the theoretical and empirical research in this paper, the overriding conclusion points to the need for organisations to consider cultural differences as a primary factor. This should be aligned with environments in which there is a need for new, secure authentication systems, where cultural considerations are necessary before the implementation of any biometric application. The success of this technology is likely to be dependent on the perceptions of the people to whom it will specifically relate.

The current social environment in which this technology operates spans participants’ perception of body scanning replacing passwords in computers and Personal Identification Numbers (PINs) in Automatic Teller Machines (ATMs). It also involves more sceptical social attitudes in which civil liberties groups point to the potential for cameras to sample physical traits. Verdi (2009) pointed to the risk of digital dossiers being compiled without responding to social fear of theft of biometric data from compromised centralised databases, raising the question as to what is so important that citizens should be willing to put that information out there. This question may be addressed in part, with an assessment of social perceptions of harm, need and psychological acceptance, to be undertaken in subsequent empirical investigation for this research.

2.14 Legal Implications
Wise (2004) pointed to the first scientific identification emerging from the work of Alphonse Bertillon (Chief Investigator for Paris Police) in the 1880s. This was followed by the emergence of fingerprint analysis in the early 1900s, recognised as having the potential to offer greater discrimination between individuals. This system continued to be relied on largely until the emergence of DNA analysis in the 1980s. Throughout the 1980s and 1990s, these two systems emerged as powerful identification mechanisms for law enforcement, setting the standard for admissibility of scientific evidence and offering guidelines for the development of biometric technology (Wise, 2004).
In 1880, the journal "Nature" had published the first use of fingerprint technology, for evidence used by Henry Faulds (Wise, 2004) but it was not specifically evident until 1892, when Sir Francis Galton published his book on fingerprints, declaring their unique and permanent characteristics. Galton established minutia, "Galton's details", subsequently used in cataloguing methods by Sir Edward Henry, in his classification system, jointly leading to the general acceptance of fingerprint technology on an international level.

The admissibility of fingerprint technology for evidence was established in the United States case Frye v US [1923] (293 F. 1013 C.D.C. Cir. 1923) using blood pressure movement to establish an early form of lie detector. But the Circuit Court rejected the reliability of this device, ruling that experts could only verify such methods if they were "generally accepted" in the scientific community. This rule was maintained for the next seventy years (Wise, 2004: 426).

Subsequently the United States Supreme Court heard the case of Daubert v Merrel Dow Pharmaceuticals in 1993, (509 US 579, 1993) replacing the "general acceptance" rule in Frye with a set of standards for the admissibility of expert evidence, including the level of scientific theory testing, subject to peer review and publication, knowledge of error rate, level of acceptance and existence of operating standards, leading to judges’ status as "gatekeepers" on questions of admissibility. This was established by the Daubert hearings for the admissibility of evidence ranging from lie detection to fingerprint and other forms of biometric identification.

From the perspective of biometrics for asylum seekers, the year 2000 saw the European Union establish Eurodac, where fingerprints of asylum seekers were initially stored on a transnational system (Council of the EU Regulation No. 2725/2000 of the 11th December 2000, concerning the establishment of Eurodac, from January 2003: cited in Petermann et al., 2006) of every asylum seeker within Europe from the age of fourteen, and also capable of apprehending illegal immigrants to the European Union; recorded in the Automated Fingerprint Identification System (AFIS). This system identified any attempt to make multiple applications, by sending the individual back to the first

In addition, the Cypriot Police National Police Force introduced The Office for Combating Cyber Crime in September 2007. This maintains close co-operation with governmental and non-governmental organizations at a National level. Furthermore, the Office sustains close co-operation with International organizations, Europol and the United States Federal Bureau of Investigation in investigating relevant cases.

Biometric data must therefore, comply with legal regulations applicable to the European Convention on Human Rights and the Human Rights Act 1998 together with the Data Protection Act 1998. The Human Rights Act 1998 specifies a general right to privacy capable of government interference only in closely regulated circumstances whilst the Data Protection Act 1998 regulates the processing of personal data through a series of principles legislating for fair and lawful use, in which individuals are informed of processes by which data will be gathered, stored and processed, at the time that it is initially made available.

2.14.1 The Legal Right to Privacy

From a legal perspective, biometric data is no more private than any other personal data. The procedure used to collect this data must be clearly communicated from its inception and its use must be shown to be objectively proportionate to its apparent benefits. Organisations must have clear strategies for collection, storage, accessing and matching of data and its use must be justified for purposes other than commercial gain (Turle, 2007). Individuals must also be convinced that the application of biometric technology will not fall victim to function creep. Individual agreement to its usage must remain consistent without the risk of changes in usage with time, leading to individual perceptions of lack of consultation and associated suspicion.
Rees (2003) suggested that stakeholders must be aware of and work towards providing uniform European guidelines in the implementation of biometric technology for authentication and verification purposes. This must comply with Article 29 Data Protection Working Party of a working document on biometrics 2003 (12168/02/EN). This recognised the sensitive nature of fingerprint and facial recognition systems in particular, regulated by the privacy safeguards introduced in Article 8 of the Data Protection Directive (95/46/EC) of specific significance in cases of fingerprint and DNA collection, where data may be obtained without the knowledge of the subject. The Working Party had specified that the biometric collection of data for access control purposes should recognise individual privacy rights. The data should be exclusively available to the user within a microchip card or mobile phone device, in the absence of central database storage. Manufacturers and suppliers must have specific knowledge of legal regulations to ensure the integrity, security and privacy of biometric systems.

In addition to public sector usage, the private sector has gained momentum in biometric use, with Turle (2007) reporting a Swiss bank in Geneva (The Pictet Cie Bank) having been one of the first such organisations to use biometric technology for access control purposes for employee management. He also cited a series of European Union-based casinos having closely followed, by implementing facial recognition systems to track and trace entrants to their premises.

On balance, both public and private sectors must ensure that the implementation of this technology is socially perceived as complying with legal rights to privacy. This may be a slow process in an environment in which individuals saw DNA database management procedures introduced in 1995 in an environment of strict control. This has been slowly eroded to a position in 2008-09 in which the United Kingdom Government was found to have breached European Human Rights legislation by retaining data taken from arrest and detention by police, irrespective of subsequent prosecution. This practise will not have assisted public confidence in the assurance that legal rights will be maintained in the technological identification of individuals within the United Kingdom.
Increasing social scepticism in this area, led the Police Information Technology Organisation (PITO) to establish a five year plan in October 2005 increasing the use of biometric technology to identify suspects more accurately (Preston, 2005). Preston (2005) considered the implementation of facial recognition systems to support traditional fingerprint scanning technology towards a strategic identification services platform (SISP). He recognised the need for the police to be assisted in improving the biometric identification of individuals associated with crime scenes and to eliminate people from enquiries.

He further argued that the combined use of fingerprint and facial technology would ensure that the right people appear in court and are subsequently imprisoned and conversely, that the right people are released. Whilst he pointed to the National Automated Fingerprint Identification System (NAFIS) having been established in March 2001, Preston (2005) suggested that an associated national facial recognition database would be beneficial, having been established in 1998 in pilot studies by Newham Council, aimed at decreasing the level of street robbery in that area.

While the perception of a surveillance state may detrimentally affect universal acceptance of this technology, within the area of passport control the United Kingdom is one of the 27 countries having signed up to the visa waiver programme (Turle, 2007). All United Kingdom passports contain a machine-readable chip, capable of scanning human features for biometric passport security applicable to all United Kingdom ports and airports.

2.14.2 The Diffusion Effect

One of the dangers associated with increasing implementation of this technology rests with the "diffusion effect." Lancaster (2009) argued that whilst the technology is currently used for four primary purposes: related to law enforcement, physical and logical access control and convenience, the on-going development of cheaper and more reliable systems will lead to its more widespread implementation in other areas of public and private sectors. In this respect, Muller (2010) extended his perception of the
application of biometrics from the established social, economic, legal and technological perspectives to those of security, privacy, interoperability and cost. This effect had been recognised by the European Commission (2005: 101) in its suggestion that:

“As biometric technologies become better, cheaper, more reliable and are used more widely for government applications, they will also be implemented in everyday life, in business, at home, in schools, and in other public sectors,” (Muller 2010: 21).

The significance of the diffusion effect has subsequently been witnessed in the implementation of biometric fingerprinting in schools, where opposition is based on the other uses associated with fingerprint scanning, related to mistrust and suspicion, rather than in the circumstances of its use in the context of registration, library borrowing and cashless catering (ICO, The use of biometrics in schools, V1.1 August 2008).

Suspicion has been raised that the use of biometrics in the school environment is a means of gaining acceptance from the younger generation towards the widespread use of government initiatives for identification cards and DNA profiling in future years. In response, the Information Commission Officer (ICO) (August 2008) suggested that legal regulation would have to complement the Data Protection Act 1998, with current data principles requiring informed consent to make suspects aware of the wider implications of biometric implementation, providing opportunities for opt-out.

In the context of biometric implementation in schools, the ICO (2008) suggested that in the absence of legislation to regulate this technology, specific data protection principles should be adhered to. This related most notably to those associated with schools’ provision for information as to why personal data is being processed. This should be supported with assurances that the data will only be used for specified purposes, with routine destruction when the pupil has left the school, together with assurances that data will be collected and stored in a secure manner. This must ensure that the risks of unauthorised access to data and loss, destruction and damage are at a minimum, fostering a general sense of the technology being implemented in a legally appropriate manner (Grijpink, 2001).
A major consideration rests with the use of biometrics for surveillance and tracking in addition to the United Kingdom regulations currently imposed by the Data Protection Act 1998. In the United States, Abernathy (2007) suggested that concern underlines constitutional protection for anonymity, both as an aspect of First Amendment freedoms of speech and as an aspect of Fourth Amendment privacy. In the context of the United Kingdom and European Union, these issues are closely linked with the regulation of human rights within the European Convention on Human Rights and Fundamental Freedoms, 1950 (as amended) and the Human Rights Act 1998.

Social perception of the protection of human rights was detrimentally affected by reported government plans to link national identification records to criminal records, to increase the efficiency of conducting background checks on people working with children and vulnerable adults (Grant, 2009). This was met with objection from privacy advocates with fears of the potential that for millions of people, identification cards would be directly linked with a detailed police record and scanning system designed to evaluate their suitability for various jobs, potentially affecting eleven million United Kingdom citizens (Guy Herbert, NO2ID General Secretary, in Grant, 2009). This may be perceived as beneficial in an area in which there is widespread recognition of the need to safeguard vulnerable members of society, but the risk of biometric data being compromised must also be seriously considered.

This concern is heightened by Fujitsu Siemens prediction that by 2013 the widespread use of biometric identification technology in the public sector, will rival that of the proposed identification card scheme, with an overall prediction that by that time, 95% of the United Kingdom population will be capable of being identified using biometric technology.

Despite the perceived risk of hacking into biometric systems, Malaysia was the first country in the world to use biometric identification cards with fingerprint technology, subsequently progressing to a centrally administered government database. Limited reading devices were distributed to citizens whilst the police were given increased reference devices, used to link individuals with watch-lists via wireless or cable to a
local terminal, to identify persons who had committed offences (de Hert, 2005). These systems are used in access control environments for public and private sectors, police forces, child care centres and retail outlets (de Hert, 2005). deHert recognised that by 2005 a number of European countries had established this controversial technology, with Spain’s national fingerprint system and France and Germany’s implementation of biometrics to credit cards and general implementation into European passport regulations in 2004, using fingerprint and facial technology, via the European Council of European Union Passport Regulations, 2004.

The legal relevance of this technology has been established primarily in the protection of data for personal information and human rights and freedoms and appreciation of the technologies that are considered to be a reliable means of maintaining security. On the question of reliability, fingerprint data is recognised as being more reliable than for example, voice recognition (de Hert, 2005), but the latter has other beneficial factors. Voice recognition is capable of identifying people from a distance and therefore useful in the context of logical access control for phone banking and associated facilities. Similarly, in large scale applications, the use of facial recognition is reported to have a failure rate of 40% (de Hert, 2005) whilst DNA remains the only identifier capable of applying uniquely to the person, but it is not considered, from a European perspective, to represent either acceptable or practical means of identification (Dorizzi, 2004).

On the question of legal compliance with privacy in the choice of storage solution, de Hert (2005) argued that the most secure method of storage rests with a de-centralised system, using smart cards. de Hert (2005) suggested that this solution offers strong security whilst maintaining privacy, in contrast to the storage of templates in a centralised system, where biometric data may be associated with other personal data relating to names and addresses, possibly leading to confusion and the risk of mis-management.

Whilst de Hert (2005) argued that with most biometric technology, no penetration of the body’s surface is required, she suggested that other, external factors may influence the legality of biometrics from a human rights perspective, specifically those relating to
reliability, proportionality, the existence of a fall-back contingency system. She further suggested that the primary consideration of government agencies and organisations should be to demonstrate a compelling reason for using this technology. In the case of it becoming compulsory for future applications, the most appropriate data should be considered as a key factor in determining whether a statutory basis is required. The primary consideration should be the extent to which it may most effectively achieve its objective of balancing security with privacy and the recognition of human rights.


In contrast to the Convention, the Data Protection legislation applies to all personal data, irrespective of private or public law applications. This legislation is also alert to new technological developments and capable of assessing the extent to which they protect the rights of consent, privacy and security for individuals and associated risks to personal liberty. These rights have subsequently been enshrined in texts produced by the Organisation for Economic Co-operation and Development (OECD), the Council of Europe with the United Nations and European Union, via the production of classic Data Protection instruments. The European Union included the right to data protection in the European Charter of Fundamental Rights (Charter of Fundamental Rights of 7th December 2000, of the European Union, Official Journal of the European Communities, C 364,2000 I, entered into force December 7th, 2000, in de Hert, 2005: 13).

On the question of data protection for storage devices, Prins (de Hert, 2005) argued that the Directive would not apply to templates on smart cards because this would not amount to identified or identifiable persons. On the contrary, the potential for smart card processors to identify smart card holders ensures that the Directive will apply, (Directive 95/46/EC, Preamble, 26: cited in de Hert, 2005).

In cases of sensitive data processing, Article 8 of the Directive identifies strict circumstances in which data may be processed; relating primarily to national security and cases in which explicit consent has been given. In respect of biometric data, blood or DNA will apply, relating to the health of natural persons in addition to fingerprint
scanning and facial recognition systems, revealing the racial and ethnic origin of such persons (de Hert, 2005). So whilst the template *per se* may never constitute personal data, storage of original scanned data on databases must comply with Article 8 of the Directive (de Hert, 2005).

de Hert (2005) suggested that the development of surveillance equipment and advanced forms of access control may be justified in their place but should be recognised against a backdrop of growing concerns of power accumulation, with policymakers in the Netherlands having stressed since 2005, that: "The Government should be intelligent but not all knowing", (de Hert, 2005: 19). This emphasises the need for society to objectively consider the legal value of accumulating vast amounts of personal information to compile databases or other government files.

de Hert (2005) suggested that compromise should be reached between legal opacity relating to privacy and instruments to stop power or to set normative limits and transparency, whereby powers are channelled according to their necessity, reasonableness and legitimacy related to the State. This approach forms a solid legal framework for normative choices to be exercised in as flexible a manner as is legally appropriate. De Hert (2005) suggested that since the events of September 11th 2001, and the subsequent development of new technology, there has been a shift from transparency to opacity when social trust has been fragile and from opacity to transparency when trust is re-established.

de Hert (2005) pointed to an example of facial recognition deployed by the Tampa Police at the Superbowl in 2001, illustrating the stealth with which biometric identification schemes could be applied. Balanced against the argument established here that vendors have a proprietary interest in keeping template algorithms secure, rest social concerns about the possibility of unethical use being made for financial gain and the risks of technical error. This may lead to the release of decrypted data by corporations and fraudulent programmers’ capability to manipulate data to support false identification matches to render false mis-matches, and government capability to force organisations to encrypt revealing personal information.
In addition, de Hert (2005) pointed to the more personal social objection to biometric images being captured and stored in cases where they, like photograph representations, may be personally embarrassing in themselves or capable of revealing unusual or distinctive characteristics, setting the individual aside from his or her peers. Here, comparison between photographs and biometric images are perhaps of greater concern, with the potential for the latter presenting irreversibility, reliability and efficiency, greater than that applying to photographic identification (Alterman, cited in de Hert, 2005).

In this respect, Karel Neuwirt (Council of Europe Report on the Protection of Personal Data with regard to the use of smart cards: cited in de Hert, 2005) argued that biometric implementation on smart cards protects the legal right of the subject in compliance with the principles of the Data Protection legislation. This suggests that individual control represents a more legally acceptable method of biometric storage towards citizens. It has the potential for consumers to be made aware of their legal rights to subsequently withdraw biometric data from a database at any time and for any reason.

2.14.4 The Retention of Data and Civil Liberties

In cases of legal challenge, Wise (2004) suggested that arguments have arisen as to the reliability of biometric technology for providing evidence. Social familiarity with DNA analysis and its representation in court, may lead to a perception of reliability but there is a risk of evidence having been falsified and of material being falsely attributed to an individual through error (Spence, cited in Wise, 2004: 28). More broadly, risks may arise from the deterioration of biometric data and its ineffective use. de Hert, (2005) pointed to the example in which the Federal Bureau of Investigation (FBI) wrongly implicated an Oregon Lawyer in the events of the Madrid bombings in 2005. De Hert (2005) argued that this was caused by a culture in which fingerprint examiners were discouraged from disagreeing with the findings of their superiors. This led to an individual being jailed for two weeks in May 2005 based upon human error rather than error in methodology or technical failure.
Cain (2002) had suggested that a significant legal development had emerged in the approach to biometrics resulting from the attacks of September 11th, 2001. Focus had shifted from legal concerns about maintaining privacy to those more closely associated with protecting society against further threat of violence, emphasising the significance of law enforcement and government access to information. But, despite societal support for legal regulation, it remains to be seen if the current Data Protection legislation prohibition on the processing of data to reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of information containing health or sex life, may need to be relaxed in the social interest of tracking terrorist groups (Cain, 2002).

From a wider social perspective in which schools have implemented fingerprint patterning for access to catering and library facilities, analysis submitted to the Scottish Government by Strathclyde University in 2009, warned that schools would not uncritically accept biometric systems (Naysmith, 2009). The report (2009) pointed to the potential danger of fostering surveillance in the younger generation, leading to social acceptance of its existence irrespective of objective justification. On balance however, it is recognised (Naysmith, 2009) that attempts to resist this technology are neither realistic nor desirable in a social context in which iris scanning and facial recognition are widely and increasingly used for border control.

Within the school environment, Boyd (cited in Naysmith, 2009) suggested that pupil take-up was enthusiastic but he acknowledged that no attempt had been made to consider the implications for civil liberties. Balanced against this, it has been stressed that the previous social stigma associated with the free provision of school meals had been eradicated by the technology, with parental consent being sought and contingencies available in cases of resistance. Overall, Boyd (cited in Naysmith, 2009) suggested that pupils were keen to use biometrics in an environment in which technology development has become the norm and in schools, akin to that implemented within airport environments.
Conversely, Geraint Bevan of No2ID Scotland, argued (cited in Naysmith, 2009) that the schools’ claim that fingerprint technology could not be reverse engineered, was untrue. He pointed to the risk of schools releasing personal records to the police and authorities in cases of request, and he argued that this may be a legal requirement in cases where data is available. Bevan (cited in Naymsith, 2009) supported suggestions from Strathclyde University that surveillance issues should be included in the school curriculum to assist staff and pupils in gaining informed knowledge of the use and civil liberties implications of this technology.

In response to these concerns, the Scottish Government published draft guidelines in 2009 for local authorities introducing biometric technology following its implementation at schools in Dumfries and Galloway and Renfrewshire. Those authorities had contended however, that biometric systems have the capacity to improve school security; arguing against criticism that they represent the emergence of a surveillance society.

Roberts (2009) pointed to the risks associated with system software to support this technology. He argued that in any identification system, from fingerprint and iris scanning to DNA profiling, computers rely on probability rather than certainty in matching samples. He suggested that the larger the sample, the less accurate matching becomes; illustrating associated risks with reliability and legal implications of such uncertainty in large-scale applications.

Despite Roberts’ (2009) argument that European Union attempts to micro manage on this issue have proved ineffective, the European Court of Human Rights clearly identified the then practise of the United Kingdom as unlawful in retaining indefinitely the fingerprint and DNA records of un-convicted suspects. It recommended that England, Wales and Northern Ireland should follow the Scottish example of deleting DNA profiles once a person is cleared or not prosecuted, except in cases of certain sexual and violent offences. Records should be capable of being stored for three years, with a further two years in the event of a judge’s consent. Support for this stemmed from European Union perceptions of DNA storage leading to subsequent convictions.
But the Nuffield Council on Bioethics and Gene Watch UK argued that DNA retention from people who were not convicted could not be justified in an environment in which a variety of other factors may have played a part (Shaw, 2008).

2.14.5 The Retention of DNA Samples

In 2008 the European Court of Human Rights ruled it unlawful for the profiles of innocent people to be retained indefinitely. Following this ruling the United Kingdom Government acknowledged a six year limit on the retention of DNA samples. Despite this, suspicion persists about government control over civil liberties. Statewatch criticised the European Union’s post 9/11 security strategy as a “frightening grab for every aspect of individual information” (Meade, 2008: 24). This report published following the 7th anniversary of the attacks on New York and Washington, entitled: “The Shape of Things to Come” (Meade, 2008) commented on a five year security strategy by the European Union as “extremely controversial”, in its co-operation with the United States towards techniques and technologies for surveillance.

Meade (2008: 25) quoted the Statewatch Report that the European Union Council will track:

“Every object the individual uses, every transaction they make and almost everywhere they go”, via a digital record: „... generating a wealth of information for public security efforts.”

Commenting on this, Tony Bunyan (in Meade, 2008: 25) said that:

“European Union standards have been by-passed or undermined and the United States of America has steadfastly refused to offer Europeans the equivalent level of privacy protection to US citizens”, arguing that this poses ever-increasing risks to our privacy and civil liberties.
Further criticisms of the European Union approach to civil liberties were voiced in 2008 by the European Data Protection Supervisor (EDPS), in his perception that the European Union approach to biometrics applied to passports in 2004. Whilst he acknowledged the Commission's provision for fall-back procedures, exempting children under the age of six and other people who were incapable of doing so, from providing fingerprint data, he argued that the measures were not good enough, when international practice set a limit of fourteen years. He further stressed the need to appreciate that reliability and accuracy of biometric technology decreases with age; suggesting that an upper limit of seventy nine years should be introduced. Significantly, the EDPS stressed that the European Commission had failed to consult with him on proposals for data processing affecting individual rights and freedoms and, that such failure had resulted in non-compliance with its legal obligation within Article 8(2) of the Convention.

On balance, Yashvan (2009) argued that biometric technology per se should not be blamed for the loss of anonymity. He pointed to the more widespread social and technological forces at work, culminating in the advancement of the computer with its propensity to erode anonymity whilst enhancing tracking and surveillance strategies. And Miller (in Yashvan, 2009) considered that even in cases of biometric data being stored in an altered form requiring complex algorithms to decipher it, the unique nature of the sample, coupled with the speed of computational technology increasingly available, renders such preventive measures irrelevant.

Willis (2009) pointed to the current social climate in which biometrics were becoming a growing part of the traveller experience; referring to the five terminals at Heathrow Airport in which iris scanning is used to allow passengers to by-pass the usual border controls. And Mine (in Wills, 2009) suggesting that biometrics has made significant moves forward in recent years in terms of reliability, accuracy and robustness, with fingerprint scanner technology having been refined to scan below the skin, in order to detect attempts to circumvent security, using of fake latex fingerprints. He further pointed to the development of technology from Japan, for palm and vein reading procedures. The perceived benefit of this rests with its unchanged status from the womb, whereas fingerprint status alters in childhood (Wills, 2009)
Further, Verdi (2009) expressed concerns about the danger of identification theft arising from biometrics and the associated implications, in which a lost passport can be replaced whereas the regaining of lost biometric identity is practically impossible. But this view has been criticised (Verdi, 2009) as revealing a basic misunderstanding of the technology, with the availability of fingerprint scanners that do not store prints on a central database where they could be subjected to mismanagement and snooping, but use a cryptic storage device on a standard personal computer (PC), which is incapable of being reconstructed to form a print.

In terms of privacy, the International Civil Aviation Organisation overseeing air travel suggested that facial recognition technology will develop to form the primary standard with fingerprint and iris scanning gaining secondary status or that of optional identification (Verdi, 2009). This pointed to the inevitability of an almost totally biometric access control route emerging in the relatively near future. Irrespective of the roles played by law enforcers, government and computer technology, Zorkadis and Donos (2004) suggested that principles of purpose and proportionality will remain. They argued that the primary consideration is to establish whether a biometric system being designed and implemented to acknowledge privacy-friendly applications is capable of minimising social risk and preventing the misuse of data.

2.15 Ethical Implications and the Impact of Computer Ethics

Jonietz (cited in Mordini and Petrini, 2007) suggested that the implementation of biometric access control traditionally raises issues for balancing individual and public rights and responsibilities, ranging from those associated with data protection and privacy, confidentiality and human rights to the liberty of the individual. The decision about taking the right course of action in any social situation is primarily based on an objective assessment of the overall benefit arising from it, irrespective of the actual outcomes of the action (Nordberg, 2008).

This philosophy supports the principle of Utilitarianism, influenced by John Stuart Mill and can perhaps be universally considered as having formed the basis of “ethical” decision-making for society as a whole. This rejects the converse approach to
consequential thinking established by ethical egoism (Nordberg, 2008) in which individuals decide on the best course of action for themselves, irrespective of the consequences for others within society.

Brady and Hatch, (cited in Walstrom, 2007) argued that the development of ethical as opposed to unethical decision making is primarily determined by individual preferences and values, with ethical practices being recognised as valuable to organisations whilst unethical behaviour has been demonstrated to cause significant losses. Ethical theories have emerged to assist in the prediction of behaviour with the conceptual framework established by Bommer et al., 1987 (cited in Walstrom, 2000) identifying six independent constructs believed to influence ethical decision making. They range from individual attributes including personal goals and motivation, personal environments and peer groups, professional standing and codes of conduct, working environments associated with corporate culture, government and legal environments with legislation and judicial systems and social environments incorporating religious, cultural and social values.

Walstrom’s (2007) study, conducted at the Illinois State University (winter 2006-2007) began with the premise that social acceptability and legality of behaviour have a relationship to the perceived ethical standing of any behaviour. Walstrom (2007) compiled thirteen scenarios to capture perceptions of social, legal and ethical issues, based on the working of Morrell. This related to information ethics, involving questionable behaviour in information, information technology and information systems. It asked questions about the extent to which the legality of behaviour links to ethical connections, and the extent to which interaction between perceived legality of behaviour and perceived social acceptability of behaviour relate to the perceived ethical connections of such behaviour. The 308 respondents in the study were gender, age and qualification neutral, with all thirteen scenarios perceived to be more negative (not ethical and / or not legal and / or not socially acceptable).

The results of the study suggested that perceived ethicalness of each scenario was related to its perceived legality (22%) more often than its perceived social acceptability.
indicating that perceived legality and perceived social acceptability have almost equal influence to the perceived ethicalness of behaviour. There were limitations however, with similar studies needing to be conducted at other institutions where social and legal environments were different, in order to determine the extent to which these findings could be generalised. Also, the nature of the study measured only perceptions rather than actual behaviour, so the “laboratory” conditions of the investigation must also be recognised. Within those confines, the study indicated that social acceptability and legality of behaviour can be influenced by informing individuals, with legal implications and social acceptability capable of being influenced by managing individuals’ expectations.

Walstrom (2007) suggested that government responses to terrorist activity since September 11th 2001 have had a significant influence on the perceptions of respondents, with the younger generation appearing willing to relinquish rights to privacy, in favour of serving the greater good of society as a whole. In Walstrom’s study (2007: 7) in 91% of scenarios, the perceived ethical correctness of the activity was positively related to the perceived social acceptability or the perceived legality of the activity, or both. Whilst government approaches may be considered a primary factor, Venier (2010) suggested that stakeholder involvement in debates about the ethical grounds for implementing biometric access control is vital, to ensure that issues of data protection, individual identity and privacy are considered by all interested parties. Venier (2010) pointed to the contribution of the European Community funded project entitled RISE (Rising Pan European and International awareness on Biometric and Security Ethics via a high level workshop taking place in Brussels in March 2010, involving policymakers, industrial players and experts from fields of academia and research from 21 countries, towards encouraging the involvement of European stakeholders. Such stakeholders included law making bodies, industry, third party privacy advocates and customers, in developing pan-European security policies to recognise the social and ethical impact of biometrics for the mobility of people and information. The project focused on minimising security and privacy risks to address the question “in what kind of society do we want to live?” above and beyond questions of which technologies may represent the best solution.
Whilst Venier’s paper (2010) focused on biometric technologies associated with travel documents, border and immigration management, it provides parallel insights into access control for workplace management. Jan Ostoia-Ostazewski and Margaritis Schinas (cited in Venier, 2010) suggest that new challenges faced by biometric implementation span the European Data Protection legal framework and the Lisbon Treaty (2009). They suggest that the “European Community” has progressed to a “Europe of Values” with values being protected by legally binding power, considering fundamental individual rights in addition to those of the common good. In support of this, Peter Hustiux (cited in Venier, 2010) focused on the privacy framework for the Stockholm programme adopted in December 2009, setting a European agenda for justice, liberty and security for 2010-2014, in which individual citizen control should be strengthened in the area of data management. But, the paper placed emphasis on the need for central data management systems to have robust protective measures associated with them, so as to avoid vulnerability to failure, disruption and malicious attack.

In applying issues of technology, emphasis has been placed on the impact of “computer ethics” as applied by traditional Western theorists, such as Kant’s Utilitarian philosophy. This considers a branch of ethics also referred to as information ethics, incorporating issues relating to information security, responsibilities of computer professionals, the merging of human bodies with machines together with concepts of robot ethics and artificial intelligence (Bynum, cited in Walstrom, 2007).

In The Human Use of Human Beings, Walstrom (2007) assessed the effects of information technology on human beings, focusing on human values relating to life, knowledge, freedom and security, in which “information ethics” is considered in a context wider than that traditionally applied to computer ethics. This led Weiner (cited in Walstrom, 2007) to refer to the “great principles of justice” upon which society should be based. Whilst Weiner’s principles spanned freedom, equality and benevolence, this thesis focuses on those issues specifically applicable to the implementation of biometric technology for access control management, considering principles of equality and the minimum infringement of freedom (Walstrom, 2007).
The above principles align with those enunciated within utilitarian philosophies in which equality is seen as having been achieved when what is just for X and Y remains just when the positions of X and Y are interchanged, with freedom and justice requiring:

"The liberty of each human being to develop his freedom to the full measure of the human possibilities embedded in him" with infringement of freedom only considered acceptable when:

"What compulsion the very existence to the community and the State may demand must be exercised in such a way as to produce no unnecessary infringement of freedom" (Walstrom, 2007).

Weiner’s methodology in developing the concept of “computer ethics” was four-fold; beginning with the identification of an ethical question or scenario relating to the integration of information technology into society, focusing on possible implications for life, security, happiness and freedom-based human values. Clarifying the ideas or principles applicable to the scenario in question, proceeding to: Applying pre-existing, ethically acceptable principles, laws and rules that govern human behaviour in society (the “received policy cluster”) (Walstrom, 2007: 7) Where ethically acceptable precedents and policies are insufficient to deal with the scenario, using human life values and principles of justice to adopt an ethically acceptable position to the given scenario.

Weiner (cited in Walstrom, 2007) further suggested that key players should influence ethical acceptance of technology within society so that those who must cope with the introduction of new technology by the nature of their role in society as computer professionals, business people, teachers, parents and public-policy makers should actively engage in information ethics to foster the acceptance of new technology in an ethically acceptable manner. Indeed, Moor (1985 in Walstrom, 2007) suggested that such influence is capable of fostering social acknowledgement that the limits of computer technology are largely the limits of individual creativity. In that respect, the
social value of implementing technology rests in the hands of individuals within society, with each holding a stake in implementing ethically acceptable policies.

Moor (cited in Walstrom, 2007) developed methodologies for individuals to refine computer ethics in areas associated with privacy and security, using the theory of "just consequentialism", combined with logical malleability, policy vacuum, conceptual muddles and core values, to solve the problem of ethical suspicion. He advocated a three-stage approach, beginning with identification of policy vacuums generated by technology, elimination of any conceptual muddles and the application of core values and ethical resources (just consequentialism) to revise existing but imperfect policies and to create new policies to eliminate vacuums and work towards establishing ethical acceptability.

Tavani and Moor (cited in Walstrom, 2007) argued against any tendency to use control mechanisms to protect privacy. They advocated the development and maintenance of "restricted access" rather than control; whilst Nissenbaum (cited in Walstrom, 2007) argued for the extension of privacy principles in public, Introna (cited in Walstrom, 2007) recognised that the rapid advance in technology, creating new possibilities for compiling, storing, accessing and analysing information, would inevitably propel philosophical debates about the meaning of privacy and the practical strategies necessary to maintain it.

2.16 Impact of Social Exclusion

The development of biometric technology has perhaps provided the most cogent example of privacy-related concerns, with its propensity to measure physical characteristics, capable of affecting the lives of more people than any other form (Wickens, 2007). Whilst the full extent of possible social exclusion resulting from the technology has not been explored, any potential for such exclusion is considered unethical, in its capacity to unfairly discriminate against people in general or within specific classes thereof.
Wickens (2007) suggested that this risk is exacerbated by no biometric match ever being perfect, with each captured template likely to be unique in nature. He pointed to the United Kingdom Passport Service trial in 2005, in which it had been established that 0.62% of a disabled sample group had been unable to enrol any biometric data, translating into approximately 62,000 United Kingdom citizens having no opportunity of being represented within the identity card legislation being proposed at that time.

Whilst he acknowledged that there appears to be no single definition of social exclusion, Wickens (2007: 52) suggested that, in the context of his research, such exclusion may be considered as “any unfair restriction or removal of access to the range of social goods and activities that other members of society do or could, take for granted.”

This definition is wide, encompassing health care, social security, employment and housing at a public policy level and the more practical issues of access to library and other social environments.

Wickens (2007) suggested that biometric technology is likely to take ten to fifteen years refinement before universal sectors of society are able to reliably enrol or verify all their data to eliminate social scepticism of this technology fostering social exclusion. He pointed to the difficulty of designing a system capable of adapting to the individual physical and behavioural characteristics of members of society. This was further highlighted in the United Kingdom Protection Services (UKPS) Biometrics Trial (Wickens, 2007) in which the technology proved incapable of dealing adequately with a range of behaviour displayed by otherwise “normal” people. This extended to enrolment and verification systems undertaken on the same day in which the systems failed to recognise minor changes in personal appearance.

In the case of facial recognition, the trial (Wickens, 2007) resulted in system failure to enrol a disabled person when s/he refused to remove a helmet and similar failure until a subject held a fringe back from her face (Wickens, 2007). Fingerprint scanning systems revealed similar inadequacies with failure to enrol subjects suffering with muscle
weakness and similar failure when a plaster had been applied to the finger presented for enrolment.

Such examples of social exclusion, apart from leading to inconvenience, can lead to stress in cases where, for example, a facial recognition at passport control falsely fails to register an individual, leading to further checks having to be conducted with immigration services. The fear of social exclusion and its implications seems only to exacerbate general social scepticism of this technology being implemented in society and risk of such scepticism will only heighten with social perception of function creep (Wickens, 2007).

The United Kingdom Protection Services (UKPS) Biometric Enrolment Trial (Wickens, 2007) selected 750 disabled subjects with an unspecified number of disabled people taking part in random selection. The results of the trial, in which fingerprint, facial and iris recognition systems were employed, revealed significantly worse problems in this sample enrolling their biometrics, from the points of accuracy and speed in enrolment and verification (Wickens, 2007). Similarly, in the case of subjects over the age of sixty, the United Kingdom Protection Services (UKPS) Trial revealed more difficulty with this age group enrolling biometric data, leading to problems associated with access to health care and social services. The development of this technology in such areas lead to support services failing to reach elderly members of society, so that risks associated with enrolment inevitably lead to this population group avoiding access to support services.

Risks of social exclusion apply more widely, according to the United Kingdom Protection Services (UKPS) Trial (Wickens, 2007) with “black” people experiencing more difficulty than other races in enrolling their biometric data for fingerprint, iris and facial recognition systems. More specific problems were identified with facial recognition of certain religious groups required by their faith to wear head and face coverings, experiencing inevitable difficulty with facial recognition systems. This leads to similar negative implications in which these groups will avoid risks of social exclusion and resultant embarrassment or offence by avoiding having to subject
themselves to social systems in which biometric technology determines access. There remains a serious risk of social exclusion with the implementation of biometric technology into society, with the three assumptions associated with this technology: that data can be collected, verified and accurately stored, having been seen to be incorrect at various levels and within a wide range of discrete groups within society.

Wickens (2007) argued that the risk of false negatives applying to such disparate sections of society, risks falling disproportionately on those groups who may be falsely denied access to health care and social security provisions to which they have traditionally been entitled. He further pointed to the importance of society fulfilling its moral duty to ensure that people are not made to suffer disproportionately as a result of the implementation of biometric or any other such technology within society.

In this respect, Wickens (2007) argued against the application of Utilitarian principles to public interest; suggesting that public interest must be assessed by considering “the balance between individuals” (Wickens, 2007: 52) so that the rights of a single individual must be balanced against the rights of other single individuals, to avoid the unfair consequence of instrumental usage. He suggested that the correct test in avoiding undue risks of social exclusion in the implementation of biometric technology is to consider whether the rights of an actual individual, if upheld, would cause greater damage to a reasonably foreseeable potential individual than to the actual individual whose rights would be overridden. This suggests that a test of this nature would work towards eliminating the unfair treatment of all individuals within society.

2.17 Theories for Conceptual Framework

The conceptual framework applied to this investigation involved a strategy in which a three-layered process was adopted in logical order:

1. Based on the Ontology of Social Constructionism: in which it is considered that “seemingly natural phenomena are not natural at all but social” (Hacking, cited in
Alvesson and Skoldberg, 2009: 31). This approach was supported with an Epistemology represented by Interpretivism: in which the social scientist is required to "grasp the subjective meaning of social action," (Bryman, 2008: 694);

2. Application of Institutional Theory: considering the structures, rules and norms established by organisations and how they are responded to within aspects of social behaviour (Scott, 2004); and the Technology Acceptance Model. The latter determines the process by which the implementation of biometric technology may be accepted by workplace members (Dimitriadis, 2006); and

3. A combination of Utilitarianism (applicable to management and workforce), Maslow's Hierarchy of Needs (applicable to the workforce) and the Psychological Contract (applicable to both management and workforce), leading to the multi-model approach discussed below:

Levels 1 and 2 of the conceptual approach considered above, lead to Level 3 (the route map for the empirical investigation) applying the Utilitarian philosophy with Maslow’s theory of Needs and the Psychological Contract. This involves a tripartite study into the social, legal and ethical impact of biometric implementation for workplace access control. It considers the theory of Utilitarianism with its application to management and the workforce, Maslow’s theory of Needs, identified within the context of workforce members and the Psychological Contract and its association with management and the workforce.

The principle of Utilitarianism suggested that the useful is the good, as elaborated by philosophers such as Jeremy Bentham and John Stuart Mill; with the aim of establishing the greatest happiness for the greatest number of people. This research investigates the moral worth of an action as determined solely by its overall utility, with the ethical perception that the value of something may be measured by its usefulness.
Maslow’s Hierarchy of Needs is considered as the second theoretical perspective in which the practical effects of biometric access control on the workforce are reviewed. This involves the examination of a needs-based framework and its impact on human motivation; focusing on the work of Abraham Maslow with emphasis on the practical, clinical experiences of humans as compared with the theory based on animal behaviour enunciated by Freud and Skinner. The proposition is that, in considering the management approach to biometric access control, managers have to find ways of motivating workplace participants in order to foster social acceptance of this technology. Maslow argued that human beings are motivated by fulfilling unsatisfied needs and that lower level needs, relating to basic physiological and safety characteristics, must be satisfied before a person will consider social and esteem needs (as first and second level needs) punctuated by the subsequent desire to fulfil the high level need for self-actualisation.

In striving to appropriately manage a workforce subjected to biometric technology, behavioural analysis of the "need pyramid" (netmba.com) is useful. Where a workplace is being introduced to access control measures, the management approach to fulfilling what Maslow described as the lowest level or physiological need must be addressed. The fundamental need for basic survival characteristics such as peace of mind can be difficult to adequately fulfil in an environment in which there is little or no evidence of dialogue between management and workforce, leading to insecurity and inability to foster peace of mind. An environment in which management clearly communicates with workplace members about issues of concern, and remains open to consultation and dialogue, will have recognised and gone some way to responding to the lower-level need of individuals to feel that they are adequately informed. Whilst this may not guarantee social acceptance, it may go some way to fulfilling the basic human need to have an informed foundation upon which to receive change of this nature and magnitude.

The Psychological Contract is the third and final theoretical perspective upon which this research is based. This theory may be applied to management and the workforce when biometric technology is used for access control. The concept of the psychological
contract emerged in the 1960s and re-emerged after the economic downturn of the early 1990s, resting on the respective expectations that people have of one another in any relationship. It considers how expectations change with time and technological development, and how fulfilment or breach of this contractual relationship impacts on respected feelings and practical responses. The objective in this research is to develop a series of Recommendations for "Best Practice", maximising the social, legal and ethical acceptance of biometric technology for access control management in a sample of United Kingdom-based organisations.
2.18 Chapter Summary and Conclusions

This chapter has considered the practical context in which biometric technology (represented by fingerprint scanning and facial recognition systems, is applied for access control in workplace environments. It has highlighted the implementation of these applications in both public and private sectors within the United Kingdom, in addition to recognising its wider international impact for border control. It discusses the benefits and risks associated with the application of biometric access control technology in the workplace, whilst recognising the perceived threats posed to civil liberties.

The chapter has balanced the perceived threats with the practical benefits secured by appropriate social, legal and ethical management, to secure both individual and collective human rights. This has formed the basis for practical auditing of biometric technology; recognising that such access control systems will only be accepted and used to their optimum if managers and recipients understand the reasons for and consequences of its use and are prepared to work flexibly to engender wider social confidence in its application.

This chapter has focused on workplace environments associated with airport security, the public sector, commercial enterprises and educational establishments. It has considered British Standards relating to the implementation of biometric technology and social perceptions towards the manner in which biometric data may be stored and retrieved. This leads to questions of the extent to which biometric technology can offer elements of privacy, personal freedom and civil liberties for implementation in workplace environments ranging time and attendance, health and safety, and incident management to guarding against the risks associated with "buddy punching."

The chapter has distinguished between instances in which biometrics may be implemented by organisations following government edict and cases in which organisations have chosen to implement such technical strategies. It has analysed the risks of theft and misuse in traditional security methods as compared with risks of biometric technology impeding civil liberties, emphasising the need for strategic change.
management approaches in each case. This has been followed with an assessment of the various academic funded projects relating to the practical management of biometric technology in the access control environment, represented by the British Security Industry Association (BSIA), and funded projects from EnCore (Ensuring Consent and Privacy), PV Nets (Privacy Value Networks), VOME (Visual and Other Methods of Exposure) and RISE (Rising Pan-European and International Awareness of Biometric and Security Ethics).
Chapter Three

The Conceptual Framework
3.1 Introduction
This chapter considers the ontological and epistemological perspectives represented by Social Constructionism and Interpretivism together with the dual principles of Institutional Theory and Technology Acceptable Models. A multi-model approach forms the basis for arriving at a conceptual framework in which principles of Utilitarianism, Needs and the Psychological Contract are applied to both management and the workforce.

3.2 The Research Path
Crotty (2003) suggested that the research path should reflect the ontological and epistemological perspectives of the researcher. This investigation is based on the ontology of Social Constructionism, in which "seemingly natural phenomena are not natural at all but social" (Hacking, cited in Alvesson and Skoldberg, 2009: 31) and the epistemological approach of Interpretivism: in which the social scientist is required to "grasp the subjective meaning of social action" (Bryman, 2008: 694). An inductive process is used to investigate four case studies, using a series of semi-structured interviews. A process of content analysis is used to reflect on participant responses, leading to the development of best practice recommendations to maximise the social, legal and ethical acceptance of biometric technology for access control management.

The Social Constructionist approach focuses on assessing the manner in which individuals seek to understand the world in which they live and work (Creswell, 2009). This suggests that subjective meanings of life experiences are developed, leading to multiple meanings in which complex views are considered rather than a compartmentalisation of categories and ideas.

The epistemological approach is based on the theoretical perspective of Interpretivism. This alludes to a process in which differences between the thoughts and feelings of individuals may be understood in the process of semi-structured interview.
3.2.1 The Ontological Perspective of the Social Constructionist

This recognises that the status of the social environment and its meanings are constantly developing in response to the actions of social beings. It applies the philosophy of Naturalism (Bryman, 2008) where the Constructionist and Interpretivist perspectives are fused. Naturalism suggests that social beings attribute meaning to observed behaviour by constructing their own social environment rather than representing a passive presence whilst the Constructionist ontology is used to portray a personal vision of social reality. This applies a process of Content Analysis in which Porter (cited in Bryman, 2008: 20) suggested that: "The world is constituted in one way or another as people talk it, write it and argue it." And Crotty (2003) argued that different people may construct meaning in different ways, despite having considered a constant phenomenon.

The semi-structured interviews for this investigation are designed with emphasis on “meaning” so that in addition to looking for patterns or themes across interviews, individual voices and stories are listened to within each interview (Denzin and Lincoln, 2008). This involves the use of a “narrative strategy” in which the responses from each interview are individually interpreted. Perceptions of social and legal compliance and ethical awareness in implementing biometric technology are individually assessed so that the rich interpretation of each participant reflects feelings and perceptions towards the research topic.

This approach supports Bamberg’s three levels of narrative positioning (cited in Denzin and Lincoln, 2008: 73) with Level I reflecting the narrator’s position of themselves towards others. Level II reflecting how narrators position themselves in relation to their audience and Level III forming an appreciation of how narrators position themselves to themselves in constructing an answer to the rhetorical question: “Who am I?” This process involves listening to the assumed positions of participants in conjunction with ambiguities and complexities within the discourse, to construct a meaningful interpretation of content analysis (Denzin and Lincoln, 2008).
The Interviews have been conducted, by gathering value-free data using an assumption of the "faceless" interviewer and respondent (Oakley, cited in Denzin and Lincoln, 2008: 135). The setting is friendly and courteous, leading to a research environment in which validity, reliability and objectivity are engendered. This approach recognises that the process of interpretation in social enquiry is never terminal or mechanical but is emergent and unfinished, leading to the generation of large volumes of data. This type of qualitative approach emphasises the need to develop a coding strategy for analysing data in a meaningful way (Bryman, 2008).

3.2.2 The Epistemological Perspective of Interpretivism

Four case studies have been selected using the Utilitarian philosophy of John Stuart Mill, Maslow’s Hierarchy of Needs and considerations grounded within the theory of the Psychological Contract. This multiple approach has sought to interpret the social meanings and perspectives of others in accordance with their individual set of meanings.

Saunders et al., (2007) suggested that this strand of Interpretivism originates from a series of intellectual perspectives ranging from phenomenology and symbolic interaction. He further suggested that the phenomenologist approach is recognised as interpreting the meaning of human behaviour in order to see things from the other person’s perspective (Bryson, 2008: 16).

This approach has supported Blumer’s (cited in Bryson, 2008: 16) theory of ‘symbolic interaction’ where individuals are understood to be continually interpreting the symbolic meaning of their environments, leading to the concept of imputed meaning. This reflects the perception of “symbolic interactionism” initiated by George Herbert Mead (cited in Bryson, 2008: 16) that our notion of “self” emerges through an appreciation of how others see us. Despite this principle having courted controversy in taking a Positivist path (Meltzer et al., cited in Bryson, 2008: 16) the general view adopted by Blumer, appears to broadly support an Interpretivist philosophy.
The link between the views of participants representing their respective roles is an essential part of the Interpretivist perspective. This is the point at which it is possible to develop a relationship of understanding the views of research subjects from their unique points of view. It challenges the concept of “generalisation” from a number of perspectives, including the need to accept constant development and refinement of biometric technology within any one organisation. It is recognised that whilst there have been organisational attempts to justify the security and integrity of this technology, each individual will have unique legal and ethical concerns. It is arguable that the philosophy of Interpretivism will most effectively cater for these complexities, in its ability to maintain flexibility in approach and analysis, through the process of understanding and practical meaning.

The theory that the research process is “bound within a set of epistemological and ontological premises which, regardless of ultimate truth or falsity, becomes partially self-validating” (Bateson, cited in Denzin and Lincoln, 2008: 31) was of great significance in this study. The empirical investigation considered this theory in assessing the perception of biometrics from the perspectives of participants towards developing an objective assessment of the social, legal and ethical requirements of those who are subjected to it.

This Interpretivist approach has presented a framework from which practical concepts have been developed towards building a series of best practice recommendations for the implementation of biometric access control technology within discrete social, legal and ethical boundaries. Whilst this strategy has placed demands on the research path both within the gathering of meaningful perspectives and the time taken to interpret responses, the end result has led to a more meaningful assessment of the links between the application of biometric technology and its practical acceptance.
3.3 The Multi-Model: Institutional Theory and the Technology Acceptance Model

The investigation uses a multi-model approach to assess the strategies applied by management to introduce biometric technology for access control and to evaluate the perceptions of the workforce towards this technology. These models have been identified, observed, tested and reviewed during the primary investigation, linking “Institutional Theory” and “Technology Acceptance.” The former considers the structures, rules and norms established by organisations and how they are responded to within aspects of social behaviour (Scott, 2004), whilst the latter determines the process by which the implementation of biometric technology may be accepted by workplace members (Dimitriadis, 2006). In addition to these models, a series of individual organisational strategies have been considered and applied within the primary investigation.
3.3.1 Institutional Theory

This theory (also referred to as adaptive theory) (Scott, 2004) focuses on the processes by which rules, norms and routines become established as authoritative guidelines for social behaviour. It further considers how these elements are created, diffused and adapted over time, towards establishing stability in social life.

Jenson, et al., (2009) argued that institutional theory has been proven to be a central analytical tool for investigating social and historical structures in the implementation of information systems. They suggest however, that it does not specifically account for how organisational actors make sense of and enact technologies in their local context. In this respect, Dornbusch and Scott (1975) examined a variety of organisations to discover differences between preferred and actual authority systems and between workers with varying degrees of power, to ascertain their preferences.

Institutional theory was further developed towards the end of the 1970s, in the work of Scott and Meyer (1970) originating from the then established paradigm of “contingency theory.” The origin of new institutional theory or neo-institutionalism had been observed in part from research in prisons where informal procedures in which inmates were actively involved, were discovered to be more effective than guard-enforced formal procedures.

In contrast, historical institutionalism is considered to have grown out of group theories established in the 1960s and 1970s, developing into concepts of incrementalisation or “muddling through” rather than rational planning. Pierson (2000) developed a concept of “path dependence” in which he pointed to the inertia of institutions, resulting in self-reinforcing systems. The Institutional Theory Model most widely applicable currently is sociological institutionalism, contrasting with historical institutionalism, with less emphasis on power and more influence on the construction of “realms of meaning”, to guide the behaviour of individuals in institutions, where change is seen as a necessary institutional process in pursuit of legitimacy.
3.3.2 The Technology Acceptance Model

This Model is meant to explain computer usage behaviour across a broad range of end-user computing applications and user populations, (Mathieson, 1991). Von Ahn (2008:3) suggested that:

“One way to model product adoption is to understand that people’s behaviours are influenced by their peers and how widespread they think a particular action is”.

3.3.3 Advantages and Disadvantages of this Model

The Technology Acceptance Model (TAM) has been recognised by practitioners and academics to explain user acceptance of information technology, but it has been suggested that the model may have a number of advantages and disadvantages in its practical application. This has emerged with observation of the process of “grouping together” multiple instruments to measure individual constructs (Davis and Venkateshi, 1996). Conversely, it has been suggested that items from different constructs should be “inter-mixed” to reduce carryover effects emerging from responses to multiple items targeting specific constructs, with the risk of the latter falsely improving the observed reliability of the process. But, the three studies involved in the research process discussed by Davis and Venkateshi (1996) in which two systems and 708 participants were involved, reported that item inter-groupings and item inter-mixing had neither a positive nor negative effect on the consistently high levels of reliability and validity arising from the Technology Acceptance Model (TAM) scales.

Evidence from this study further suggested that verbal evaluations reported greater subject confusion and anxiety when items were inter-mixed than when they were grouped together. This led to a general indication of the value of the Technology Acceptance Model (TAM) strategy in using the original grouped format to identify practical user acceptance of information technology.
3.3.4 Practical Application of the Technology Acceptance Model

A pilot study was conducted in 2004, to consider the usability of biometric access control in a stadium hosting athletic events. It focused on system security, performance and acceptance (Dimitriades and Polemi, 2004). The model was based on Amberg et al., (cited in Dimitriades and Polemi, 2004)) Dynamic Acceptance Model for the Re-evaluation of Technologies (DART) incorporating perceived ease of use, usefulness, network effects and cost. This model was considered in the primary study conducted for the current research, focusing on approaches taken by management in implementing biometric access control and assessing perceptions of workplace participants. Dimitriades and Polemi (2004) investigated participants’ attitudes towards biometrics and those specifically relating to BioAthletics. Their research was conducted in three phases: using questionnaires before and after informing the user of the operation of BioAthletics. The questionnaire was subsequently repeated after the user was enrolled and had tested the system in question.

Dimitriades and Polemi (2004) reported that, at phase one, the acceptance of biometrics was relatively high, with acceptance reaching higher levels still at phase two. They suggested that this was based on concerns having been minimised after users had been informed of the operation of the system and assured that smartcards containing their biometric data would store information in encrypted form. They were further assured that there would be no central storage of this data on any database. At this stage, participants reported recognition of the benefits of the system and its potential to increase security levels without compromising usability and privacy at the time of attending athletics events.

3.4 The Framework for Investigation

The Theoretical Framework for this investigation involves a tripartite study into the social, legal and ethical impact of biometric implementation for workplace access control. It considers the principle of Utilitarianism towards management and the workforce, Maslow’s Hierarchy of Needs, within the context of workforce members and
the concept of the Psychological Contract within management and representatives of the workforce.

3.4.1 The Utilitarian Philosophy (applicable to Management and the Workforce)

Proponents of this philosophy such as Jeremy Bentham and John Stuart Mill considered that the useful is the good. Its aim is to establish the greatest happiness for the greatest number of people. The Utilitarian philosophy also considers the moral value of an action as determined by its contribution to the overall social sense of utility (Regan, 1980). This philosophy is based on the premise that action should be assessed as being positive based upon the proportion of people in whom it produces happiness and overall welfare. It also assimilates Utilitarianism to utility in its practical and functional (as opposed to its theoretical) sense. In this respect, a Utilitarian artefact consists of a practical item in support of social good, used to assist people in taking care of their basic needs (Smart and Williams, 1973).

Whilst this philosophy is generally recognised within the social setting associated with the current investigation, its limitations have also been considered. One of the main objections to Utilitarianism rests with an interpretation that it may be incompatible with justice. This perception arises from the assessment of Utilitarianism as proposing that, in some circumstances, it may be justified to treat people unfairly. This is based on the anecdotal assumption that the gaining of some social benefit for X (for example, relief from poverty) may be achieved by imposing on Y a less extensive disadvantage (associated with social deprivation) and no other option arises in preference to this situation. This leads to the assumption that Utility is arrived at by the option chosen above producing more Utility for X than the deprivation imposed on Y (Williams, 1973). In this respect, Mill suggested that the perception of unfairness may manifest itself where the sentiment of justice feels more socially compelling and more authoritative than the sentiment of benevolence associated with it (Smart and Williams, 1973).
In assessment of the nature, value and limitations of the Utilitarian philosophy, this research advocates the overall value of Utilitarianism, focusing on the moral worth of an action being determined solely by its overall utility, with the ethical perception that the value of something may be measured by its usefulness.

A multiple case study has been conducted to investigate management approaches to implement biometrics as an access control route to the workplace, measured against any scepticism workplace participants may feel towards this technology. Management have been required to illustrate the practical utility of this type of access control as opposed to paying lip-service to issues of security and reliability. The investigation considers whether management strategies have complied with the doctrine in which acts are taken to be right solely insofar as their consequences maximise overall happiness.

The investigation has assessed workforce perceptions of change and consequence from a behavioural perspective. Inalhan (2009) argued that when established working patterns are broken, new connections must be fostered. These are put in place to support workplace participants so that management communication strategies outlining the reasons for introducing biometric technology for access control, can be objectively assessed (Mazumdar, cited in Inalhan, 2009). Mazumdar (1992) suggested that if little thought is given to the way in which these changes may be perceived by the workforce, this can result in negative effects on performance, leading to long-term damage to working relations. Management must be aware that one third of major change initiatives fail because employees and associated personnel are resistant to change (Strebel, 1998 in Inalhan, 2009) rendering the formation of appropriate management strategies of paramount importance.

Inadequate management support has the potential to adversely affect productivity and morale leading to poor attitudes towards organisational strategies. This may last for months or years, extending to the risk of loss of key personnel and perhaps more seriously, attempts to sabotage the change (Attwood, cited in Inalhan, 2009). With workplace participants being linked to their environment through attachment, familiarity and identity, any strategy attempting to change this is likely to be met with
an emotional response. This may lead to a sense of alienation that may have long-term adverse effects for the internal security of the working environment, (Inalhan, 2009).

Inalhan (2009) used a social constructionist approach to assess how workplace participants perceive the introduction of new workplace strategies and how they develop an objective understanding of associated implications. Inalhan (2009) used "Interpretative phenomenological analysis" (IPA) to analyse and interpret the qualitative data generated from his investigation.

Whilst it was suggested that workplace participants have to adapt to more complex and diverse settings, many attempts to introduce new workplace strategies have failed due to universal participant resistance to change (Stegmeier, cited in Inalhan, 2009). This has led to a suggested "phasing strategy" with the philosophy enunciated that: "all action is for the sake of some end and rules of action.... must take their whole character....from the end to which they are subservient" (Mill, 1863:1).

The management approach to communicating the need for biometric technology in the access control environment, whether for security, reliability or to ensure knowledge, is paramount in establishing workplace acceptance and support.

Mill (1863:2) further suggested that:

"Men's sentiments, both of favour and of aversion, are greatly influenced by what they suppose to be the effects of things upon their happiness, the principle of utility, or, as Bentham latterly called it, the greatest happiness principle." This is interpreted in the Metaphysics of Ethics by Immanuel Kant, as: "....so act that the rule on which thou actest would admit of being adopted as a law by all rational beings." (Mill, 1863: 3).

This suggests that the role of management is powerful in establishing moral conscience in the majority of the workforce, to comply with what is considered to be objectively rational behaviour. If we take this philosophy to its ultimate end, there is supposition that majority compliance inevitably leads to the "Utilitarian or Happiness Theory." This suggests that whatever can be proved to be good must be so by being shown to be a means to something admitted to be good without proof (Mill, 1863:3).
Whilst the Utilitarian principle of happiness for the majority is a persuasive philosophy, questions of semantics in analysing "benefit" from both management and workplace perspectives may be less clear, specifically when balancing arguments of security against the possibility of relinquishing individual rights and liberties. In this respect, Arneson (2004: 1) suggested that Utilitarianism may be incompatible with justice, implying that there are circumstances in which we should treat people unfairly or "violate their moral rights.” In response to this, Mill argued that:

“Justice implies something which is not only right to do, and wrong not to do, but which some individual person can claim from us as his moral right” (Arneson, 2004:49).

But, justice theorist would say that we should count as positive the reason for a policy, only that it satisfies legitimate interests (Arneson, 2004). The consultation process between management and workforce is paramount in establishing a legitimate case for the implementation of technology and encouraging workforce acceptance on questions of social, legal and ethical utility.

3.4.2 Maslow’s Theory of Needs (applicable to the Workforce)

The second theoretical perspective has considered a needs-based framework and its impact on human motivation. This has focused on the work of Abraham Maslow with emphasis on the practical, clinical experiences of humans as compared with the theory based on animal behaviour enunciated by Freud and Skinner.

The proposition is that, in considering the management approach to biometric access control, managers have to find ways of motivating workplace participants in order to foster social acceptance of this technology. Maslow argued that human beings are motivated by fulfilling unsatisfied needs. He argued that needs relating to basic physiological and safety characteristics, must be satisfied before a person will consider social and esteem needs (as first and second level needs) punctuated by the subsequent desire to fulfil the high level need for self-actualisation.

In striving to appropriately manage a workforce subject to biometric technology, behavioural analysis of the “need pyramid” (Neher, 1991) is useful. Where a workplace
is being introduced to access control measures, the management approach to fulfilling what Maslow described as the lowest level or physiological need must be addressed. It is proposed that the fundamental need for basic survival characteristics such as peace of mind, are difficult to adequately fulfil in an environment in which there is little or no evidence of dialogue between management and workforce. This leads to insecurity and an inability to foster peace of mind. So, an environment in which management clearly communicates with workplace members about issues of concern, and remains open to consultation and dialogue, will have gone some way to responding to the lower-level need of individuals to feel that they are adequately informed. Whilst this may not guarantee social acceptance, it will go some way to fulfilling the basic human need to have an informed foundation upon which to respond to change of this nature and magnitude.

The nature of biometric technology and historical intervention in the workplace tends to be founded upon the concept of security. In engaging in dialogue with the workforce, management may address the need for this technology to be imposed upon members of the workforce. The manner in which security issues are justified, will determine the extent to which the second low-level need of the workforce is fulfilled. Once basic physiological needs are met, the next consideration will be to concentrate on safety and security, leading to freedom from the threat of physical and emotional harm.

When the basic need for access control has been identified, management have to address the first level of the higher social need. This involves the construction of a group-based dynamic where the workforce is encouraged to work together to ensure that safety and security are maintained. There must also be an assurance of general, if not universal, social acceptance. The key to fostering this position rests with management assurance that privacy and basic human rights of the individual will not be disregarded in the process of implementing and using this technology. It will be difficult to engender social acceptance in an environment in which the individual considers that s/he has sacrificed basic human rights.
Social conscience is linked with what Maslow described as the second higher level or individual self-esteem. This rests on the need to develop a sense of importance within the group dynamic. This was identified by Maslow as a sense of "belonging", in which a combination of attention, recognition and self respect are ensured in the manner in which the workforce is required to accept and respond to the implementation of technical developments.

Whilst the highest or summit need identified by Maslow rests with self-actualisation or a sense of experiencing periods of profound happiness and harmony, he recognised that only a small percentage of the population reaches this level. Whilst management would aim for this level of social acceptance, in reality it is achieved in few instances. But, despite the relatively few people striving for self-actualisation, those who do so must be identified and responded to appropriately. Maslow suggested that when self-actualizers do not have this need fulfilled, they respond with meta-pathologies or persistent problems. This often leads to a sense of despair, alienation and cynicism; which can have an adversely negative effect on other members of the workplace.

In aspiring to social, legal and ethical acceptance of change, management must recognise the individual needs of the workforce. This will involve acknowledging the needs level at which individuals are operating. It will also involve recognition that needs may be used as levers of workplace motivation as opposed to securing self-actualisation and universal acceptance from the entire workforce. The difficulty with the universal application of "need" however, rests with the fact that some cultures will prioritise it differently to others. This may lead to management response varying depending on the cultural norms of the workplace.

The current research has been conducted from a United Kingdom perspective. The investigation has tested Maslow’s theory in the light of what has become an increasingly multi-cultural Britain. This suggests that the application of the Motivational Triangle or Pyramid introduced by Maslow may be challenged. In response to this, the ERG (Existence, Relatedness, and Growth) developed by Clayton Alderfer, in 1969, as a needs-based model was considered in this investigation. The
major difference in approach rests in Alderfer’s philosophy that more than one need may be motivated at any one time and that higher needs may be addressed before lower needs are fulfilled.

The ERG theory makes allowances for different need priorities based on culture, providing a more flexible approach, recognising and responding to a wide range of observed behaviours. This theory also introduced the “frustration-regression” principle in which, when higher-order needs are not fulfilled, individuals may regress to lower needs to increase their overall satisfaction at a lower-level. This theory differs significantly from that of Maslow in suggesting that management strategies, in which one need is focused on at a time to the exclusion of all others, will not effectively motivate the workforce.

Perhaps most significantly the ERG theory recognises the impact of frustration-regression on motivating the workplace. If individuals are not provided with opportunities to grow, and reach a state of complete acceptance, from social, legal and ethical perspectives, they may regress to fulfil practical relatedness needs. These needs may be associated with more stringent acknowledgement of the practical implications of this technology. General social acceptance may be achieved only with individual need for greater management dialogue or workplace incentives, perhaps associated with an increase in pay or some other incentive.

Having considered the theories developed by Abraham Maslow in 1943 and Clayton Alderfer in 1969, the empirical investigation in this research has addressed and analysed parallels and differences in individual perceptions of need. These theories have been considered in the development of a series of recommendations to maximise acceptance of biometric technology within specific working environments.
3.4.3 The Psychological Contract (applicable to Management and the Workforce)

The third and final theoretical perspective upon which this research is based considers the concept and effect of the psychological contract on management and the workforce when biometric technology is used for access control. The concept of the psychological contract emerged in the 1960s and re-emerged after the economic downturn of the early 1990s, resting on the respective expectations that people have of one another in any relationship. It considers how expectations change with time and technological development, and how fulfilment or breach of this contractual relationship impacts on respected feelings and practical responses.

In applying this concept to the relationship between management and workforce, Wellin (2008) suggested that the question of whether words articulated by management are borne out by management actions, is significant. Wellin (2008) illustrated an example in context from the Pret a Manger chain of food outlets in which the psychological contract is implemented within the organisation’s business model. This sets out its expectations for workplace members balanced against the reasonable expectations of the workplace towards the organisation. The role of the psychological contract within this example illustrates an element of forward-thinking and diversity. It recognises management goals of social responsibility and equality and provides a platform from which this organisation appreciates that management and workforce have mutual expectations that may be fulfilled in practise, using an appropriate business model.

This approach to the management and workforce relationship is capable of being applied to cases in which access control technology is implemented within a workplace previously familiar with less perceived intrusion. At the point of introducing such technology, acknowledgement of the pressure and impact of the psychological contract can form the basis for management to enter into dialogue with workplace members, to establish social, legal and ethical acceptance of practises.

Contracts of employment may set out the beliefs employees have about the implementation of the contract between themselves and their employers but they are not
explicit, written or legally binding in nature. Irrespective of form or legal influence it is suggested (personneltoday.com) that the psychological contract forms the foundation for clarifying employees’ practical perceptions of “give and take” in the working environment. It encompasses the practical understanding of employee well-being, attitude and performance. These are essential considerations in environments in which technology has developed, with the psychological contract playing a major role in enhancing trust to foster social, legal and ethical acceptance of emerging workplace practices.

The subjective nature of this relationship acknowledges different perceptions for each individual. This is an important factor in the objective analysis of social and ethical perceptions where age, culture and role may lead to very different approaches. Management must subsequently respond in an individual way. Whilst it may appear necessary to formalise the psychological contract in order to clearly negotiate its terms, employers will have difficulty making clear and binding promises in areas relating to new and developing technologies where it is unclear how the future application will unfold.

Emphasis must be taken away from formality in order to foster individuality. There will be incidents in which management practices and promises will fail or operate at a lower level than perceived as acceptable to the workforce. This may strengthen the relationship between management and workforce, if it is handled in an environment of transparency and consultation. Employers may use a range of attitudinal and behavioural approaches for involving employees in the decision-making process; through regular face to face meetings. This will encourage employees to provide feedback on their attitudes towards the implementation and management of biometric implementation.

This process may be coupled with the distribution of attitude surveys to gain a more general interpretation of employees’ attitudes towards technological developments in the workplace. However this is achieved, whether formal or informal, the process of
two-way communication between management and workforce is essential to the development of mutual trust, with its focus on people rather than technology. The link between Maslow’s Theory of Needs in employee environments and the mutual relationship established in the psychological contract is evident. There is a nexus between the individual need for recognition and the communication of business strategies between management and individual members of the workforce. This will lead the workforce to foster a sense of being integrated into the organisational plan. This strategy will achieve the best return from workforce energies and foster openness to accepting new challenges. It will avoid any tendency of management to instil a sense of fear for security in the workforce. This approach is most likely to achieve practical and long-standing trust and acceptance of this technology.

The psychological contract may be an important tool in a business case for incorporating effective people management policies and practise into the change management process. This approach must however, be fostered at an early stage in the decision-making process, combined with practical implementation of technology in order for it to be socially, legally and ethically accepted by the workforce.

This thesis has focused on the extent to which workplace members socially, legally and ethically responded to the implementation of biometric technology for workplace management. The combination of Utilitarianism, Need and Psychological Contract may assist in maintaining practical acceptance involving transparent consultation and dialogue between management and workforce. This will play an important role in recognising how acceptance is fostered and working towards more widespread implementation of this technology in future years.
3.5 Application of Theoretical Perspectives to Research Objectives

The first and second objectives were:

1. To undertake an investigation into the development and perception of biometric technology involving fingerprint and facial recognition systems for access control to workplace environments, by means of a critical literature review.

2. To assemble representative case studies, combining the conceptual framework of Utilitarianism, Need and Psychological Contract by undertaking semi-structured interviews with management.

Consideration of these objectives began with an explanation of the inductive (theory building) approach to this research path. Bryman (2009) described this approach as one in which the relationship between theory and research is recognised, where theory is generated out of the process of investigation. This is undertaken in qualitative research with emphasis on gaining an understanding of the meaning people attach to events as they arise.

This approach presents a flexible structure in which changes in emphasis during the progress of the research, may be recognised and responded to within the investigation (Saunders et al., 2007). It moves from individual observation to statements of general themes or laws, (Collis et al., 2009). Theoretical perspectives are developed from the observation of empirical reality, leading to the deduction of generalised inferences from specific events and experiences. The general purpose of the investigation is assessed to discover “what is happening; to seek new insights; to ask questions and to assess phenomenon in a new light” (Robson, cited in Bryman, 2009: 133).

An exploratory study was used to assess of the nature of the problem under investigation. The study used literature searches whilst interviewing those who were experts in the field of biometric implementation. This strategy adds weight to the
flexible nature of the research, where exploration may lead to new insights being established. It recognises that focus may begin in a relatively broad way and become narrower with the progression of the research (Adams and Schvaneveldt, cited in Saunders et al., 2007: 134).

3.5.1 Approach to Case Studies
Creswell (2009) defines case studies as a strategy of enquiry in which a programme, event, activity or process of one or more individuals is explored in depth. The timescale to achieve this objective spanned April 2010-January 2011, following a pilot study undertaken in April 2009.

The case study strategy was considered to be suitable to the current investigation into a range of biometric technologies, their implementation and usage. The study involved organisations, companies and individuals in a number of contrasting cases but each were studied in a similar manner (Ticehurst and Veal, 2000). It used a collective approach in which a series of cases were considered with the aim of investigating a general principle (Silverman, 2005), relating to the social, legal and ethical impact of biometric technologies within the cases in question. The selection method involved "theoretical or purposive sampling" (Mason, cited in Silverman, 2005: 130) where organisations were studied together, based on associated interest groups and individuals, all of whom had links with the implementation and use of this technology. This approach assisted in linking individual responses with a pre-set theoretical position in order to formulate an explanation of the issues being investigated.

The research area called for an investigation into the "how" and the "why", with the case studies considering holistic, meaningful characteristics of real life processes and associated responses. Yin (2003) supported this approach in explanatory investigation, challenging the view of some sceptical social scientists (Shavelson and Townes cited in Yin 2003). The latter had argued that case studies are appropriate only for the exploratory phase of an investigation with the experiment being necessary for explanatory phases.
In contrast, Yin (1981) favoured the use of different investigative strategies. He argued that case study and experiment are inclusive or pluristic, with each strategy being appropriate for exploration, description and explanation. The only point of danger may arise where the researcher designs one strategy whilst being aware that another is more appropriate to the research path.

The design of the case studies and subsequent interviews expanded the theories established in the literature review. The benefit of the case study rested with its ability to illuminate a decision or set of decisions in order to establish why they were taken, how they were implemented and with what result (Yin, 2003). This is the essence of the current research process, with its objective to investigate the implementation and effects of applying biometric technology in a socially acceptable manner.

The use of multiple case studies was also based on the theory that this approach explains the causal links in real-life interventions that are too complicated for experiment (Yin, 2003). Emphasis was placed on the construction of validity (both internal and external) and reliability. The case study was linked to a conceptual framework (Markus, cited in Yin, 2003) in order to show why the technology in question was implemented and received in a specific social way. This was achieved by analysing a blend of concepts from the principle of the Psychological Contract, Maslow’s Hierarchy of Needs with Jeremy Bentham and John Stuart Mill’s principle of Utilitarianism.

The first concept considered the existence and nature of the Psychological Contract. This assessed the relationship between management perceptions of need in implementing biometric technology and the practical perceptions of the workforce. The Psychological Contract, in comparison with the contract of employment, is not legally binding. It focuses on capturing employee perceptions of what they believe they will get in response to what they give and analysing the extent to which this may influence social behaviour.
The effect of the Psychological Contract links with Maslow’s Theory of Human Motivation, where he argued that low-level needs associated for example with safety, must be satisfied before higher end needs, such as self-fulfilment are pursued. This investigation examines low-level human perceptions of security and safety before considering the possible implications of implementing biometric technology on a wider scale and fulfilling the needs of society as a whole.

John Stuart Mill’s view of Utilitarianism stemmed from the perception that: “it is expecting too much to require that people shall always act from the inducement of promoting the general interest in society” (Mill, 2008: 16).

This was the basis for the case study method conducted in the primary investigation for this research. The interview process aimed to probe reasons for societal acceptance or rejection of a technology that appeared to be universally publicised as in the interest of preserving security for all. Focus was placed on an assessment of Mill’s Harm Principle:

“That the only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others” (Mill, 2008: 12).

Conversely the primary investigation examined the philosophy in which personal interest is not a decisive factor in our expectation of societal acceptance, neither is any encouragement to conform based on the proposition of greater happiness or ethical conformity. Whilst Mill (2008) recognised that this is the basis on which individuals may be encouraged to conform, he recognised also that they should not be compelled to do so. The primary investigation included query about how management communication with those subject to biometric implementation, may affect responses to the application of this technology within society. In doing so, it recognised that specific management strategies may yield diverse responses.

Given the multiple nature of the case study approach, a process of generalising from case study to theory was undertaken in order to reach some consensus in the social perception of biometric implementation. This culminated in the development of a series
of recommendations to maximise acceptance of biometric access control for workplace management.

3.5.2 The Cases

The investigation considered four cases (multiple case study design) with each organisation being the subject of an individual study but with the study as a whole representing consensus within several organisations. This "embedded" approach was argued to represent a more compelling strategy than that adopted in a single study, resulting in a more robust collection of data (Yin, 2003). It used a process of replication logic, where from the four cases under investigation, two were literally replicated where similar results are predicted. The remaining two cases were theoretically replicated, predicting the generation of contrasting results.

Jacob Neilson (1994) had commented on the emergence of saturation point in the research process. In his approach to User Testing (useit.com) he argued that the application of three components from representative users, representative tasks and observation, applied to a sample of at least five individual participants, is sufficient to form a representative sample. Neilson (1994) suggested that as the data group grows beyond this sample, less is learned about the set because findings will begin to repeat themselves. He argued that a draft series of recommendations may emerge from this sample. This may be followed by a new process, subject to further testing to discover the effect of the original findings where new problems may emerge with the new design.

The value of the second drafting of recommendations allows for deeper consideration of issues associated with social acceptance of the technology under investigation. This results in more detailed understanding of the issues and further refinement of the recommendations.
The rich context of the data generated from this approach assisted in the construction of more representative series of recommendations arising from the research process. But care had to be taken to avoid any suggestion that results, conclusions or theory generated from the research could be universally applied, to avoid compromising any subsequent question of external validity (Saunders et al., 2007).

The primary method of investigation involved semi-structured interviews with management in the workplace. This was intended to be conversational as opposed to structured query (Rubin and Rubin, cited in Yin, 2003) focusing on two distinct tasks. The tasks were to follow the line of enquiry based on research protocol and to ask questions in a conversational yet non-biased way. Becker (cited in Yin, 2003) suggested that the “why” question should be replaced with the non-threatening “how” question.

Creswell (2009) suggested that the interview should follow a pre-defined protocol beginning with a heading (date, place, interviewer and interviewee) and instructions for the interviewer to follow so that interviews are standardised throughout the research process. There should be an ice-breaker question in introduction, followed by 4 or 5 questions and sub-questions. The interview should end with a concluding question or statement, with probes for 4 or 5 questions for participants to explain their responses in further detail. There should be space between questions to record responses with a final statement of thanks to acknowledge the time and effort of the participant / informant in addressing the interview questions.

The process of recording the data gathered from the empirical study, took the form of blended electronic and hand recorded processes. Emphasis was placed on avoiding causing anxiety to participants and this perspective was also considered in the nature of the questions asked, when they referred to personal and sensitive subject areas (Blaxter et al., 2002).

Lists of prompts or reminders were used in the interview. The prompts considered management relationships with the workforce, the working environment and communication strategies (Gillham, 2005). Consistency in process was ensured with the
use of the same questions in each interview. This was based on Gillhams’ (2005) philosophy that the semi-structured interview benefits from well-targeted questions recognised as being more stimulating to research participants, resulting in a more vigorous and robust response.

1. To compile an audit of current practice, involving a series of semi-structured interviews with sample organisations, in order to collect data and undertake content analyses associated with practical implementation strategies. This focused on theories of Utilitarianism, Need and the Psychological Contract within the context of biometric access control; whilst

2. To synthesise empirical investigation via the compilation of a first cut series of Recommendations for “Best Practice” to maximise the acceptance of biometric access control. Examples of good practice were generated from secondary and empirical studies, using semi-structured interviews with participant organisations. This focused on participants’ perceptions of Need in responding to biometric access control and the impact of the Psychological Contract; and

3. To generate a working series of Recommendations for “Best Practice” for dissemination to participant organisations for consideration and feedback.

Following the compilation of a first-cut series of Recommendations, semi-structured interviews were conducted with selected “stakeholders” and participants. This involved an assessment of first impressions from a sample of management and workforce towards the suggestions compiled within the initial Recommendations.

This method introduced a quantitative approach to the traditionally qualitative research process, Woolcott (2001). He had suggested that all research has observation at its foundation and this traditionally qualitative method should recognise that most
qualitative researchers would benefit from maintaining an open mind to areas in which counting and measurement may be necessary.

In contrast, Blaxter et al., (2001: 77) defined survey research as;

".... a method of collecting information by asking a set of pre-formulated questions in a pre-determined sequence in a structured questionnaire, to a sample of individuals drawn so as to be representative of a defined population", but there are both advantages and disadvantages of applying this method to the research process.

The advantages include the opportunity to design questions so that answers from individual surveys can be added together to produce results applying to the whole sample. This would involve semi-structured interviews applying to a sample of respondents. This approach was not favoured however, due to the data being prone to represent mere snapshots rather than focusing on specific processes and changes. The nature of the interview questions may also preclude the checking of participant understanding and the survey may rely for validity on breadth rather than depth. (Blaxter et al., 2001)

It was recognised that there may have been opportunities for structured interview questions to set boundaries in timescales and geographical perspectives. But, on balance, the decision to conduct semi-structured interviews to achieve the fourth objective was based on justification for the same questions to be asked in the same order, using an interview schedule, (Bryman, 2008). The purpose of this was to address specific issues and responses from those subjected to access control systems. These responses formed the basis for a first cut series of Recommendations for organisations identified within the investigation, using Maslow’s Hierarchy of Needs and Motivation together with the Psychological Contract.

The semi-structured interview questions attempted to capture opinions and attitudes of respondents in their every-day exposure to access control technology. They were conducted with a sample of participants chosen from previous workplace members using a combination of face to face, email and telephone discussion, depending on the
availability of respondents. Again, in each case the questions were standard, with identical questions being asked of all respondents (Maylor and Blackmon, 2005). The object of this approach was to ensure that the data collection process was consistent across interviews. This worked to eliminate the risk of different approaches being taken in the research path and to ensure that consistency was maintained in confirming the social, legal and ethical requirements of all participants.

A neutral stance was established in the research path, whereby a “balanced rapport” was adopted with the participants. The research was conducted in the manner of a theoretical script establishing the role of “interested listener”. The interview responses were recorded in a pre-agreed coding scheme, with a balance being struck between rewarding the participants’ efforts and avoiding any evaluation of responses (Denzin and Lincoln, 2008: 125).

3.5.3 Risks Emerging from the Interview Process

Denzin and Lincoln (2008) pointed to three sources of error that may emerge from the interview process. They ranged from the respondent attempting to please the interviewer and providing misleading information, leading to relevant information being omitted. The second error may emerge from the administrative process itself or the choice of question sequence. Thirdly, error may arise from confusion in the interview technique resulting in a detrimental effect on clear communication of the questions. The possibility of errors was fully considered in this research prior to administration, in an attempt to eliminate as much risk as possible.

The interview process was piloted in March 2009 and it was revised accordingly. This process began with an initial request outlining the objectives of the interview seeking to ensure that the respondents were clear about the confidential nature of the process. Questions were piloted for inconsistency and misunderstanding, with an assessment of the amount of time needed to complete the interview response form or instrument.
Having piloted questions and addressed data collection, recording and retrieval strategies, amendments were made to ensure that the process was as efficient and accurate as possible, prior to live interviews being conducted. At this point, an objective assessment of appropriate sampling was necessary in order to ensure that accurate conclusions could be drawn about the social unit under investigation. This supported Maylor and Blackmon’s (2005) suggestion that, in order to effectively sample, there must be a clear understanding of the population being sampled and the characteristics being measured.

The sampling frame for this interview was represented by members of the workforce subject to biometric access control systems within selected organisations and institutions. The characteristics for measurement involved an assessment of theoretical perspectives relating to Maslow’s Hierarchy of Needs and Motivation and the social perception of the Psychological Contract. The interview approach ensured that it was representative of the population under investigation so that the chosen sample was unbiased and a reliable source of data, capable of being generalised from the sample population.

A process of random sampling was used for the ultimate investigation, recognising that time and financial constraints would lead to there being a greater chance of selecting some units for investigation than others. In contrast, the pilot interview had involved convenience sampling, in which the sample was chosen based on ease of access. This is an appropriate strategy for the piloting stage of the investigation but it is impractical in actual terms, where the research method must ensure that general and academically robust conclusions can be drawn from the sampling process.

The exercise following the pilot interview involved snowball sampling in which the convenience sample selected for the pilot interview suggested further contacts from the original participants observed within the research setting. Whilst issues remained with drawing general conclusions from the sample, the snowball strategy was recognised as an effective way of studying a social network of this nature. Indeed, O’Leary (cited in Maylor and Blackmon, 2005) suggested that qualitative researchers are often more
interested in the lessons learnt from the sample than how well the sample represents the population under investigation.

Following the compilation of initial Recommendations, a process of iteration, was undertaken, in which an alternative random sample of participants was chosen to repeat the exercise of semi-structured interviews undertaken for the fourth objective.

This involved the evaluating links between primary responses and existing international codes, using semi-structured interviews with a selection of management and workforce. This involved the use of content analysis in compiling a series of Recommendations based on theories of Utilitarianism, Need and the Psychological Contract, towards a practical assessment of the research question:

*How should organisations using biometric access control systems, implement procedures to address social, legal and ethical concerns in the workplace management of specific environments in the United Kingdom?*

This objective focused on the rationale for conducting a final set of interview sessions with both management and workforce. Subsequent content analysis was undertaken, to form a consensus of response based on the theoretical perspectives of Utilitarianism, Needs, Motivation and the concept of the Psychological Contract. This approach clarified and refined the first cut Recommendations focusing on the search for structures and patterns emerging within the texts and making inferences based on their regularity (Myers, 2009).

The process began by reviewing the primary data in order to develop a set category of words and phrases relating to social, legal and ethical aspects of biometric technology for access control management. It was followed by a coding of the text in preparation for subsequent analysis. McNabb (cited in Myers, 2009) suggested that the advantage of this method rests with its ability to present the structure and interpretation of text in a clear and concise way. He recognised however, that the disadvantage of this approach rests in its tendency to compartmentalise pieces of information from the content in which they were originally applied, hampering the quality of contextual meaning.
In response to this, the process of content analysis was carefully considered with the frequency of words and phrases being identified throughout the research process. This resulted in an effective method of analysing such large volumes of data. Mostyn (cited in Collis and Hussey, 2009: 164) defined this process as the “diagnostic tool of the qualitative researcher, which they use when faced with a mass of open-ended material to make sense of.”

This approach led to a process for systematically converting qualitative data into numeric data. This resulted in a more efficient method by which the Recommendations could be compiled to respond to the social, legal and ethical issues identified most commonly by research participants.

This strategy began with a process of reviewing and identifying a representative and manageable sample from the four case studies investigated. This led to the development of a series of coding units (represented by words or phrases) or themes established within the data, supporting the strategy of Collis and Hussey (2009). They had suggested that coding units can be transcribed into a coding frame where appropriate coding units can emerge from words or phrases, themes or documents (Collis and Hussey, 2009).

The current research path did not support the suggestion of Collis and Hussey (2009) however, that the Positivist paradigm would commonly be used, in which further analysis would be undertaken in a statistical way. In contrast, the current approach adopted an Interpretivist method to develop a list of Recommendations to maximise acceptance. This approach was based on a qualitative method, termed by Altheide (cited in Bryman, 2008: 276): “ethnographic content analysis”, in which emphasis is placed on the role of the researcher in constructing the meaning of the texts. In this approach, categories are taken to emerge out of the data, resulting in the development and eventual analysis of “meaning in context”.

In preparing for this process of analysis, all forms of primary investigation were carefully analysed. This process began with separate semi-structured interviews with
management and the workforce followed by a semi-structured interview with management and the workforce combined. During the first three stages, preparation was undertaken for the drafting of a first cut series of Recommendations, with refined suggestions emerging from the combination of semi-structured interview with management and workforce. This was supported with content analysis, provided a triangulation of the perception of all parties towards social legal and ethical use of biometric technology for access control.

Prior to the formal reporting of analysis this material was piloted in order that any difficulty in applying the pilot scheme would be identified at an early stage. The risk to reliability in coding, based on possible inconsistencies in inter-coding and intra-coding, did not pose a concern in this process because the design and coding phases were undertaken personally. This assisted in an assurance of reliability on consistency of approach having been adopted in earlier semi-structured interviews (Bryman, 2008).

The advantage of using content analysis in this study rested primarily with the transparency of the coding scheme, allowing for ease of replication and resulting in an objective approach to analysis. It was recognised however that this largely qualitative study is unlikely to yield the same results in subsequent cases. But, its reaching of a point of theoretical saturation (Maylor and Blackmon, 2005) in which meta-level objectives were achieved, yielded results in which the main findings should be fairly robust.

In terms of generalisibility, the multiple case study approach may not be representative of all samples of biometric technology for access control. The series of Recommendations arising from this investigation however, should provide opportunities for findings in similar investigations to yield similar results. This must be supported however with an appreciation of different environmental factors regulating the social, legal and ethical frameworks.

This is a vital consideration in establishing credibility in the research process. It recognises the importance of findings being clearly presented with academic and
practical evidence to establish transparency in appropriate circumstances. This will test the practicality and value of the Recommendations generated for implementation in similar access control environments within the United Kingdom.

3.6 Chapter Summary and Conclusions

This chapter has considered the perspectives of ontology and epistemology associated with Social Constructionism and Interpretivism. It has linked these perspectives with the dual principles of Institutional Theory and Technology Acceptable Models, in discussing the empirical investigation for this study. A multi-model approach has formed the basis for arriving at a conceptual framework in which the principles of Utilitarianism, Needs and the Psychological Contract have been applied to management and the workforce.

An inductive approach has been discussed, involving semi-structured interviews being conducted with four case studies, leading to a series of best practice recommendations to maximise the social, legal and ethical acceptance of biometric technology for access control management.
Chapter Four

Research Approaches (Actualisation)
4.1 Introduction

This chapter discusses the unit of analysis chosen for the investigations that of multiple-embedded case studies, in which semi-structured interviews are conducted across a range of organisations. This process discusses the use of multiple informants, in which a variety of viewpoints (at both management and workforce levels) are identified and analysed. The chapter also considers the advantages and disadvantages of the case study, recognising that whilst it is practical, the case study is inherently difficult to gain access to in a consistent way. On balance, however, when this approach has been carefully constructed and piloted, the chapter recognises that well designed case study data leads to the effective testing of concepts and theories in their natural environments. This may lead to the development of a “best practice” approach in pilot and subsequent empirical studies.

4.2 Choosing an appropriate Unit of Analysis

In identifying a suitable unit of analysis, emphasis is placed on credibility (Collis and Hussey, 2009) to ensure that the sample is appropriately identified in conjunction with the research objectives. This is established using a series of semi-structured interviews, in which data is collected personally and transferred into electronic format before embarking on content analysis.

The need to ensure that the research process is systematic, rigorous and well documented cannot be over-emphasised in establishing dependability, but Collis and Hussey (2009: 182) referred to three additional criteria for consideration. They considered “saturation, meaning in context and recurrent patterning.” Saturation involves complete immersion into the research process, whilst meaning in context considers the extent to which the data is understandable within holistic contexts. Recurrent patterning considers the repetition of experiences, expressions, events or patterns of sequenced behaviour throughout the process of investigation. This continues to the point of theoretical saturation (Bryman, 2008) with emerging concepts having been fully explored to the point at which no new insights are being generated.
The current research involves a process of *convenience sampling*. The sample frame is established using industry and academic contacts emerging from attendance at security conferences in conjunction with contacts established from academic sources. This approach has progressed to an element of *snowball sampling*, in which initial contacts have developed into networks, to identify and refine appropriate case study participants (Maylor and Blackmon, 2005). This networking strategy was considered appropriate to the Interpretivist approach conducted in this study. Here academic and management contacts together with manufacturers and suppliers of biometric technology were identified at an early stage in the research process, for their experience of the phenomenon under investigation (Collis and Hussey, 2009).
Figure 3: Choosing the Unit of Analysis

Dr. Fred Preston (Sagem), Professor Ross Anderson (Security Engineering), Marek Rejman-Greene (Home Office) & Professor Juliet Lodge (Leeds University)

Professor Leslie Worrall (Coventry University) – Technology Acceptance Model and Institutional Theory & Phil Booth (No2ID)

Sureyya Cansoy & Carla Baker (Association for Biometrics), Professor Mike Fairhurst & Professor Mark Nixon (European Biometric Forum)

FIELD WORK – Educational Establishment, Local Government Department, Public Communications & Aviation
4.3 The Use of Multiple-Embedded Case Studies

Collis and Hussey (2003) considered the case study as representing an extensive examination of a single instance or a phenomenon of interest using phenomenological methodology. The current investigation has used a combination of experimental and explanatory approaches. The former examines issues experienced in introducing new technology into organisations and evaluating its effects, whilst the latter applies existing theory to explain what is happening in the practical context.

This research path examines opportunist case studies through access to specific people and businesses using academic and commercial contacts from the university environment and beyond. Collis and Hussey (2009) suggested that the value of this approach rests with its potential to develop stimulating and original responses, despite the research being limited to specific instances of organisational experience. In contrast, Maylor and Blackmon (2005: 243) did not consider the case study approach to be “pure” research method. They saw this approach as a “bounded entity, studied in detail with a variety of methods, over an extended period.” Whilst Yin (1994) suggested that the use of case studies to answer a range of exploratory, descriptive and analytical research questions assists in both theory testing and theory building approaches.

The scope of the current investigation was widened from a single case to multiple studies in order to apply them to similar and dissimilar samples. This has presented an opportunity to extend and modify essential theories. A series of data collection and interpretation strategies have been combined, using semi-structured interviews and cross-case content analysis, to identify common and disparate issues across cases and to determine common patterns.

The analysis process has quoted extensively from content established through interviews, both face to face and in electronic format. Experiences of history and future are determined to clarify perceptions set within an Interpretivist paradigm, as opposed to the theoretical framework associated with the Positivist approach.
The interviews have been transcribed as early as possible within the data collection process. Field notes and transcripts were initially read through without any detail, after which the process was repeated with more detailed interpretation. Specific notes of meaning and interest were made in margins, using key words and phrases ready for further transcription into indices. Codes or indices were revisited via transcripts, to identify repetition of and relationships between themes, where connections were further coded. This led to the emergence of more general theoretical ideas and concepts but the importance of maintaining a perspective in coding was recognised, in the generation of reliable data upon which the process of Content Analysis could develop (Bryman, 2008).

This research focuses on empiricism, relying on the proposition that concepts apply to or derive from experiences. This supports the theory that elements within the world have truth or merit only when they can be related to an individual’s experience. The interviews have placed emphasis on the individual experiences and views of participants from both organisational and workplace perspectives.

In order to achieve the research objectives, emphasis is placed on Weber’s (cited in Crotty, 2003: 67) interpretation of “Verstehen” or understanding as opposed to “Erklären’s” process of explanation. The former occupies a primary place in human and social sciences, with natural science focusing on consistencies or scientific “laws” (nomos). Conversely, human issues of explanation concentrate on specific cases (idios), focusing on the unique development of individuals. But Weber (cited in Crotty, 2003: 68) considered that this distinction is unnecessary and that the scientific method is sufficient to apply to two forms of science, catering for both nomothetic and idiographic inquiry.

In the current investigation Weber’s all-encompassing approach is not supported. Instead, emphasis is placed on the importance of the social world and the unique characteristics propounded by each participant. In contrast, an approach towards investigation in the “natural world” would be represented by quantifiable methods. This research path disagrees with Weber’s approach in which he argues against the
generally accepted position that human and social sciences require methods differently to those adopted for the natural sciences.

The approach taken in this study supports Blaikie (cited in Crotty, 2003) recognising the fundamental difference between the subject matter of the natural and social sciences. However, Crotty (2003) suggested that studies of the natural and social sciences have moved closer together by recognising the un-sustainability of the Positivist approach to objectivity. This has led to observations of natural sciences being themselves social constructions and human interpretations. This position supports a combination of Constructionism and Interpretivism akin to the methodological approaches developed in the current research.

Mead’s theory of Symbolic Interactionism (cited in Crotty, 2003) originated from teachings at the University of Chicago and it was later supported by Blumer (cited in Crotty, 2003:72) within three interactionist assumptions. This began with a theory that:

"humans act towards things on the basis of meanings that these things have for them"; that “meaning is derived from and arises out of, social interaction that one has with one’s fellows” and “that these meanings are handled in, and modified through, an interpretive process used by the person dealing with the things s/he encounters” (cited in Crotty, 2003: 72).

In the current investigation the three elements of Symbolic Interactionism have formed a foundation from which semi-structured interviews focus on the Interpretivist philosophy of investigation. This has stemmed from organisational approaches to biometrics and enquiry into the perceptions of individuals who were subjects of this technology, with emphasis on social, legal and ethical principles. This approach has used Peirce’s (cited in Crotty, 2003: 73) interpretation of “pragmatism” in which he focuses on methods of reflection leading to the development of clear ideas. This was later recognised in Williams James’ work (cited in Crotty, 2003: 73) as looking away from individual “categories” to focus on “consequences and facts”.

The current investigation works towards developing of a series of best practice recommendations for use in participant organisations, based on collaboration between
all interested parties. Thayer supported this approach (cited in Crotty, 2003:73) in its capability to align "pragmatism" to the ordinary situations in which actions occur. This research focuses on forging a link between the interpretation of biometric technology and its impact on the social environment, forming the basis for the development of a series of socially acceptable recommendations.

In considering the interview process, Dewey (cited in Crotty, 2003: 74) emphasized "culture" as opposed to "experience" as a significant factor. This was supported by Mead's (cited in Crotty, 2003: 74) assertion that in our graduation to 'personhood', we must be able to take the role of others. This process begins with that of play in childhood where children assume the role of others in developing their perceptions towards "generalised others." This leads to the development of broader social awareness or "symbolic interaction".

The current research emerges with an investigation into the "perception" of human rights and attitudes towards the protection of liberties and an assessment of ways in which biometric technology may compromise feelings of intrusion on privacy and integrity. The empirical study has recorded the meanings of participants (Mitchell cited in Crotty, 2003). Dialogue is used to develop perceptions of cultural differences in individual participants. The study does not question underlying culture but examines the cultural perspectives of others in order to reach an interpretive assessment of their perspectives, using an ethnographic strategy. In this respect, the semi-structured interview has been designed with the aim of "getting inside the way in which each participant sees the world" (paraphrased from Hammersley, cited in Crotty, 2003: 76).

This process may also be undertaken using unstructured interviews, according to Crotty (2003) but the current study has chosen a series of semi-structured interviews to form a boundary whilst maintaining sight of the subjective experiences of respondents. In doing so a balance has been reached to avoid the risk of arriving at an overly subjective approach.
4.4 Case Study Design

The process began by identifying case studies to decide on the most appropriate type of data to collect and the most effective methods of data analysis. Maylor and Blackmon (2005) suggested that the decision about appropriate types of cases should focus on how they can be identified. This may be achieved by determining manageable and justifiable boundaries and deciding whether cases should be associated with pre-existing theoretical categories. They suggested that often researchers may not fully understand the cases before they write up the results.

Whilst a single case study is appropriate for investigating a single unit of analysis, the current investigation uses a multiple approach to distinguish between issues that are unique to an individual case and those that are common across cases. But this approach establishes patterns and uses individual cases to support or deny propositions, it provides less opportunity for concentrating on specific issues within each case. This formed the rationale for the current investigation using an embedded approach, in which studies of multiple roles within organisations have been investigated, to establish patterns of behaviour and practice.

Maylor and Blackmon (2005) suggested that between two and eight case studies should be conducted, ensuring that each case is investigated in appropriate depth. They also suggested that a single in-depth case study may be conducted, supported by a number of smaller cases. They argued that the contribution of each new case should be reviewed to the point at which no new information is being added, to avoid instances in which a final review may reveal that findings were the same in all cases.

This multiple case study approach focuses on the generalisation of chosen cases to theory, rather than to a sample of similar cases. In the current investigation a combination of responses are examined, from those using or having used the technology to those considering doing so and those not having done so. Maylor and Blackmon (2005) support this approach suggesting that it begins with loosely defined objectives that evolve according to the data collected.
The current investigation has taken the multiple case study approach defined by Pettigrew and Whipp (cited in Bryman, 2008). They had examined a series of United Kingdom-based companies including successful and unsuccessful examples from three sectors, to establish common and differentiating factors influencing the successful process of change management. Similarly, the case study analysis in the current investigation begins with the writing up of a detailed study for each case associated with the research. This leads to narrative established from the perceptions of each participant, leading to content analysis, where a series of patterns are identified across cases, using cross-case analysis.

Conclusions are drawn by selecting specific categories and identifying how each case is aligned to the categories, in terms of their similarity or dissimilarity. Common themes are identified across cases, determining those that most strongly illustrate each chosen theme, recognising that the research has taken a systematic path, with a clear story and conclusions. This approach establishes an appreciation of social, legal and ethical perceptions of the technology in question.

The multiple informant approach, in which participants from management and workforce are asked the same questions, has fostered confidence that the answers to questions are generally representative of the research population. The investigation has also placed emphasis on multiple viewpoints (both organisational and workforce-based) in which care has been taken to ensure that the "company line" does not overwhelm the research findings, leading to the generation of unreliable data.
Figure 4: Multiple Case Studies

Methodology (Multiple Case Studies)

- Semi-structured Interviews
- Interview Responses (Management & Workforce)

Presentation and Analysis of Multiple Responses – First Cut Recommendations (Case Studies A-D)

Selected Case Studies (A & C) – Recommendations sent with Suggested Best Practice

Analysis of Feedback from First Cut Suggestions & Compilation of Recommendations for "Best Practice Model"

Educational Institution, Local Government Department, Public Communications and Civil Aviation

Educational Institution and Public Communications
4.5 Advantages and Disadvantages of the Case Study Approach

The multiple case study approach has a number of positive and negative effects. Positive effects range from the confidence fostered in data interpretation and conclusions. Negative effects range from the time-consuming nature of multiple cases and difficulty in reconciling answers from different methods, leading to incompatible results. But Maylor and Blackmon (2005) suggested that such drawbacks would balance with the process of triangulation, to lend greater reliability and value to the research.

Myers (2009) suggested that one of the most significant advantages of the case study approach is that researchers can use it to explore theories in a practical, real-life setting in which they are able to maintain close contact with the research environment. Against this rests the main disadvantage, that there is often difficulty in gaining access to the participants necessary to engage in meaningful research. Organisations may initially respond in a positive way but upon reflection, commercial priority may lead to the research process being perceived as taking too much organisational time. There may also be concerns about the practical effect of the research, leading to conclusions that may detrimentally affect business reputation.

The process of finding suitable organisations and gaining appropriate permission to conduct research may be prohibitively time-consuming. This may lead to delays in the research process and, in extreme cases, the necessity to re-design the research agenda.

Balanced against the disadvantages, however, Myers (2009) suggested that researchers determined to pursue the case study method, find the process rewarding, providing opportunities to empirically test concepts and theories within their natural settings.

4.6 The Concept of “Best Practice”

In the context of establishing and maintaining a process of “best practice” in empirical strategy, the Oxford English Dictionary (867) refers to “Good Practice” as “satisfactory procedure”, as opposed to the process of “Best Practice” suggested in this study. In the context of this investigation, “Best Practice” may apply to the process
by which organisations balance unique features with those it has in common with other organisations.

Whilst "Best Practice" may be achieved by replicating procedures traditionally established in other circumstances with other groups of people over a period of time, it should not be considered static, but should be recognised as being subject to evolution with time. In the current study, this may lead to the emergence of new processes to secure access control in workplace environments; resulting in the development of "Evolving" as opposed to "Best Practice".

4.7 Piloting

Silverman (2010) suggested that a system of piloting or trying out different styles of questioning prior to the primary investigation is a feature of good research. This process has the advantage of assisting in forming appropriate questions developing interview schedules, and Silverman (2010) suggested that this relative inexperience can assist in generating interesting data.

In the current investigation, the major piloting exercise undertaken for the study has been considered. The pilot took place with a practitioner having both industrial and academic experience in the field of biometric systems with a variety of manufacturers and suppliers of biometric access control technology for workplace management.

4.7.1 The Pilot Case Study: Sagem Securite (Basingstoke)

Contact was made with the research participant (Dr. Fred Preston, United Kingdom Director of Identification and Management Solutions at Sagem Securite, United Kingdom in Basingstoke, England) following a Biometrics Conference held in London in July 2008. The participant delivered a paper at the 2008 conference dealing with the "Practical Aspects of Using Biometrics for Identity Assurance". Contact was subsequently made via email in February 2009 in order to ascertain the suitability of developing a case study about Sagem, using a semi-structured interview as a pilot
exercise. Following a favourable response the piloting schedule was set with associated deadlines.

The Schedule for the pilot study and associated procedures was emailed to the participant in February 2009 when communication was made to set the boundaries for the case study. This included an explanation of the data collection plan and agreement towards a mutually acceptable time for the visit and duration of the interview. An assessment of the main documents associated with the research, including ISO/IEC TR 24714-1: 2008 relating to Jurisdictional and Societal Implications of Commercial Applications was undertaken before the visit. This document was analysed before designing and drafting the semi-structured interview questions. The issues for interview discussion were then prepared and finalised during March 2009.

At the beginning of the interview, the themes for the case study and associated protocol were introduced. The nature of the research path and plans for collaboration with sample participants were outlined together with the planning procedure and strategy for achieving the first objective set for the research path.

4.7.2 Statement of Purpose:

To investigate the development and perception of biometric implementation in a sample of United Kingdom-based organisations via an assessment of fingerprint and facial recognition in workplace management recognition for access control systems.

4.7.3 Extract from the Pilot Interview and Participant Responses:

The following represents an extract of the framework questions and salient issues arising during the pilot interview:
1. How has Biometric technology developed at Sagem?

“Right, well um, the link between Motorola and biometrics? Well I guess it started in round about the late 1990s when Motorola took over a company called Printrack. This was a specialist biometric company providing mainly, not exclusively, but mainly, fingerprint ID systems for law enforcement and that’s where much of the automation, if you like, in biometric ID has come from. There has been a long history of mention about fingerprints associated with law enforcement so, getting back to your question, Motorola took over Printrack in (I think) the year 2000 and evolved into wider biometric ID for assurance of ID really, safeguard of ID etc. It went from ID management to ID assurance which is elements of ID.”

2. What would you consider to be your past and current (personal) perceptions of biometric technology?

“I don’t think it’s changed for me personally. I have always associated fingerprints with law enforcement but actually, speaking personally, I have no wish for this or any other biometric to be used for any other application provided (and this is not just because we are talking about this area) but I really strongly believe in a few key things and that is the right protection of data that’s involved, what the data could be used for and what the data (either implicitly or explicitly) tells you about the person involved. By this I mean that there are some biometrics that actively implicates the person in areas that are otherwise personal.”

3. Could you expand on that for me briefly please?

“Well, classically fingerprints don’t tell you much about a person at all. I mean, they’re individual to the person as you know, they are very individual but they don’t actually tell you much about them. Arguably, let’s go perhaps to the other end of the scale; currently in terms of current technology we should perhaps mention DNA, although some people would not call that biometric. Let’s illustrate: DNA will tell you a huge amount about the person. It may be that in time, DNA will come under the definition of biometric technology in terms of automation of the person but also it may be that analysis of, for instance, iris pattern or, conceivably, types and combinations of ridge structures on fingerprints, may tell you more about than simply that they are individual to that person... in terms (I don’t know) of height, weight, propensity for whatever... medical /mental condition or those aspects... they are absolutely key.

Um, it is a concern because it is difficult to see exactly where that will go but I’m very much a pragmatist in the sense that we do, throughout our lives, many things.... We balance risk against benefit, even to the extent perhaps of using one’s credit card. I mean, there’s perceived benefit there and there may be an unseen risk or maybe there’s a perceived risk. People have a different balance on these things and a different understanding but, getting back to the biometrics, in the sense of using biometrics to help one do things – to get benefit, whether that may be convenience or actual financial benefit. I am very pragmatic about it personally and I think that many people are, from the more modern applications that we’re seeing.”
You think that “many people” are pragmatic about the need for this technology? Could you explain this a bit further for me please?

“I think it was the late 1990’s. I still do give presentations and I normally throw in a quote I made many times, that biometrics is going to become an integral part of our lives.... and I still believe that and I think that’s going to grow up and become more and more an everyday event... not necessarily (I see that happening but I don’t see a need) but I do see it happening and I think there is an age thing, a generation thing, Dare I say it...books are going out and the internet is in. It’s the keyboard; it’s the screen and things like that for the younger generation. Web-cam, facial image, that sort of contact is very difficult. I have no figures to substantiate this but the impression is that the younger generation are far less concerned about downloading what the older generation may consider to be personal information... the classic is Face-book....everybody quotes that.”

You mentioned that the technology was becoming an everyday event but you felt that there was no “need” for this. Could you explain this a little further for me please?

“I think, to me, biometrics is relatively new. I mean, I could also argue that it has been around for absolutely ages, but in the sense we’re talking, it’s a relatively new technology (if I could use that word in this context)...and it tends to be sexy and the perception is that it’s the answer to all your problems, whereas in fact, it may not be and in many cases, it isn’t, but nevertheless there are applications where the user / client / customer want biometrics as a solution but there may be some better solutions possibly.”

4. To what extent do you have concerns about implementation issues, and what types of concerns arise?

“Leaving aside the IT – to get a working system one always has to consider that what biometrics or indeed combinations of biometrics that one attempts to use, there are always going to be exception conditions. There will be people who, for whatever reason, cannot, will not or have great difficulty in being a donor,...through no fault of their own or (in a sense) the technology....that’s just life. So I think the key thing is that when I stand and talk to people about this, I always stress the exception conditions. For security of course, the exception conditions are the weak point in that there is always a way around it. This does not refer to biometrics but if I forget my PIN, how do I gain access to the building and what’s the token? If you can’t donate your biometrics or have used your fingerprint perfectly OK for the last three years but have recently suffered a gardening accident, are you going to be denied access to your place of work? Those aspects really need consideration and the people issues, business processes around that.

Another one of my mantras is that biometric technology is only a small part of the system... so one has to consider issues such as buzz phrases e.g. ‘the enterprise issue’ or ‘the end-to-end process’, the business processes around that ... the biometrics have to fit
into. Sometimes they fit in very well and sometimes they don’t but those issues are very important. And all the practical issues of... I’m not actually sure, even though I’m in the business, if that is a story around something that never happened (an urban myth) or technical myth... implementing a fingerprint reader for access to a car is all very well, but if you’re in Alaska or in the desert or your finger gets stuck to the car or you can’t remove your gloves etc.... there are a huge number of practical issues in terms of the environment and far less extreme than that... you can take a facial image, but what’s the background? What’s the lighting like? Is it dark? Is it misty? Is it light? You have glasses on, I have glasses on etc. People do the most amazing things, we all know that. Whatever you think they’re going to do, a huge percentage will. A few people will use the equipment totally differently and approach it differently. One can only pick that out by experience of actually doing it, because it is very difficult to predict.”

5. Who are your major customers / clients?

“Very largely public sector – that’s the market we’re in... Law enforcement, Government applications, visas, passports, ID schemes etc on a national or at least a wide-scale.”

6. In your experience, what types of technology are most commonly implemented or acquired? For example, would you consider multi modal and multi factor technology to be common?

“You may consider multi-modal and multi-factor technology as common but I’m not sure that’s the way the trend is going, but I would certainly advocate it. To set against that of course, you need to start looking at some of the real applications.... combinations and indeed can one afford it? I’m afraid money does reign, it’s a balance against cost and effectiveness but I would advocate multi modal because, not only does that give you the potential ability to reduce the (so called) errors, but also an ability to have an alternative should a problem happen. If you have a preferred biometric and a problem with injury – facial image, iris and glasses, facial hair, suntan, make-up, cut when shaving etc..... so there is a gender thing here that tends to come in as well. Systems sensitive to false positives and false negatives tend to be at the leading edge of technology associated with higher quality or effort that’s been put into, and then they are going to be more expensive.

I would add risk to that and the critical point of user-friendliness, usability, intuitive use etc. Most customers are sufficiently savvy to realise that it is risky rejecting somebody...in terms of customer annoyance etc and these issues would all come under ‘risk’, together with jargon terms fostering further annoyance for habitual or non-habitual users. For example, the first time you go to an ATM it always takes longer because you are reading specifics, but if you have used it many times..... This gives the implementers some interesting design issues because, for the first time user you are
going to have to instruct them through step by step, but if you have an habitual use, some of those intermediate instructions can be really annoying, especially if they slow you down, you will want to skip them. You can design around that but it does give some interesting design issues.

The main types of technology we’re involved in are fingerprint and facial image. Fingerprint relates back to law enforcement – over 100 years of that and automation is at least 30 or 40 years strong. In terms of research, there is a huge amount of research gone on in that time. I would advocate that when one goes home to one’s loved ones; you don’t take them by the hand and look at their fingerprints to acknowledge who they are. I would advocate on a human basis, facial recognition, possibly gait, body stature and all those other biometrics are hugely important for a human but not such in an automated way. So fingerprints have had a huge amount of development in the sense that that is very strong technology and absolutely key technology for law enforcement in virtually every country in the world.

With facial recognition, much of research and development is going into this because of course it’s non-intrusive and you can do it at a greater distance, so it is considered as up and coming technology. It is good but it needs to get allot better before the sorts of applications that people, the average customer, expects it will work in. Against some of the other technologies, iris especially has great application to things like access control and people doing it at greater distances. You don’t have to necessarily be in a specific spot. So face and iris are very prevalent because they are surface technologies that aren’t intrusive and can be done at a distance without contact. So, to me, they are the key ones....What is somewhat different, more disappointing from the technical point of view is voice recognition. If it worked well, you could do it remotely by telephone or other communication channels, like mobile. You wouldn’t need any other technology because mobiles are prevalent and (I haven’t mentioned spoofing) that gets back to the risk-benefit curve of what biometrics may be used for what applications. There isn’t a single biometric for all applications; some are better than others for all kinds of reasons.”

You mention that you don’t consider voice recognition to be reliable? Could you tell me more about that please? Are you thinking of the Harrow Council example for instance?

“Personal ID tells us allot about what biometrics says about a person – or not. Probably a cold, toothache etc could affect reliability. Some voice recognition systems see through that but certainly, in the battle scenario, when a pilot is trying to use all his senses to control a plane for instance.....it’s an interesting issue. Also in the case of legal evidence....this is a fascinating angle, introducing another difference between biometric technologies. Historically fingerprints are established but there are fewer facial recognition experts.... and, in the case of iris scanning....computer may say no! These are interesting points from the perspective of legal experts.”
Yes, are you thinking of the relatively recent admission of computer-generated evidence in court perhaps?

“I believe this is time for a European law to be introduced. If you’re going to deprive somebody of their liberty, for example, lock them up in prison, you have to have a human involved. In the United Kingdom, that is interpreted, in fingerprint terms, of having an expert rather than a machine say: “this is a match.” So...I’m not sure what that means for iris scanning or whether the human involved is involved in court. I’m not sure how s/he interprets that....”

Perhaps program developers analysing such biometric technology may represent the “human” element?

“Different applications make biometrics all very different, which makes this a wonderful area to study.”

You said you wanted to be reminded to mention “spoofing”?

“Only in that it is my belief that you can spoof ANY biometrics given enough effort. Whether you can detect that spoof afterwards is a matter of measure....things are advancing all the time. But... again it gets back to implementing the system against the current requirements.

On a technical level, it gets back really to analysing what you’re doing and analysing the danger and knowing what the error rates are likely to be. A classic case of implementing something against the correct requirements was, not picking on, but illustrating this by a case in Japan, where a lady got through the border a number of times using a plastic glove (if you like) using imitation fingerprints...because she was being asked the wrong thing. They were asking: is this person on our database? The fingerprint she was using wasn’t but they should have been asking: has this person enrolled before, and who is this person? So they were doing a “watch list” check...so the system worked but it didn’t ask the right question”.

7. To what extent does Sagem deal with biometrics for Access Control systems?

“Not strictly access control – more in terms of law enforcement and the enrolment / duplication and management of national scale (databases of individual biometrics) by which I mean, they could be driving licences, for instance, national ID cards or passport information...or benefit information. We have a system that uses, or customers use, fingerprints for access to benefits.”
8. What are your personal perceptions of the Social / Legal and Ethical impact of this technology?

"If I concentrate on the question of ID cards for UK citizens.....I must stress that this is not a Motorola view but my personal view is that, we have a history in the UK, for whatever reason, of not wanting to carry an ID card, in the sense perhaps of wanting freedom to be a person. That is not to say unnecessary but there is of course the issue that we all carry ID documents most of the time, for lots of different reasons, and so I don’t see a problem with an ID card, but there is allot of media focus on the token and not the card itself, which, to my mind, is a bit irrelevant. It is really what one does with the data, how we manage the data, that is absolutely crucial. It is media focus on Government protection (or not) of personal data that feeds the anti-ID lobby and so you can perhaps understand that view."

9. To what extent are there “common” methods available to solve the issues you have discussed?

"Um....I’m mentally hesitating to scope this! Through the development of biometrics there are individual, small problems....some potentially show stoppers however!...but they have been solved and some solved by the natural evolution of technology and some solved specifically, for example, there are readers that will detect “liveness” or work very well in bright sunlight, or under water, or work if the finger is sweaty or whatever. Of course, camera technology is (mobile phones with at least 3 mega pixel seems to be crucial these days)...so that sort of imaging technology linked with communication – band width increase – transmission, assurance of data, PKI...things like that, all those go together...not specifically biometric but used to overcome some of the issues there.

I think still there is a concept of some people with ethnic backgrounds, for example, not wishing to touch things per se, despite the fact that they do so anyway, and a combination of people who really do associate fingerprints with criminality and therefore would not wish fingerprints to be used for any application other than law enforcement and criminal justice, so there are those issues, and....to get back to one of my mantras now....we have gone from using technology in a very static way (when we have had to be stationary to use it) or to go there, with going through a period of somewhat mobility, where the device can actually come to the person or can be hand-held. But...we’re rapidly heading, and this is where the technology is going, is actually development of ID on the move.

This poses some interesting technical issues about border crossing or going into a building where you have to channel people, at football grounds, why go through a turn-style? Or, you don’t have to stop at the turn-style and put your card in, or on the Underground (currently using the Oyster card) may not be biometric but “near field” communication where you literally don’t have to stop. Consider the standard credit card with magnetic strip, signature and contact less chip or for example, pay-wave technology, currently used at Costa Coffee (associated with the Oyster Card); this is contact less but not biometric currently, although it could become so in the future. So...you don’t HAVE to involve biometrics. Credit cards are the shape they are because of reading machines whereas if contact less, it could be any shape or size etc. It could
be a watch, mobile phone...anything you use... The Japanese currently sell for example, key-rings in the shape of a doll and they market clothes for it!"

10. With reference to the ISO / IEC TR 24714-1:2008 (Information Technology – Biometrics – Jurisdiction and Societal Consideration for Commercial Applications) is there perhaps a need for something more specific, to foster social acceptance? Can the United Kingdom work with this standard in the absence of specific European or domestic legislation?

“We need to get more mature about what we are trying to do and why we’re trying to do it. The problem with Standards is that they often lag behind the technology and they deliberately avoid the issues of why you’re trying to do this...so, not easy. But,...it is something we can work with...but it needs improving and bolstering. One of the efforts in this field (many people, countries, politics and agenda involved) but one of the efforts attempted at the moment is Best Practice processes and procedures of countries at border crossing...because they are very high level. If you look at meta-level it looks simple but it isn't because of people. We are talking about human beings here so I think there is allot more to be done.”

4.8 Concluding Comments on the Pilot Interview

The pilot interview set the scene for deciding on the rationale for choice of case study participants, their status, location and technological implementation strategies. It involved less structure and a more prolonged approach to questions of implementation and response. This resulted in the development of more focused issues in the interviews, designed to achieve the objective of the initial investigation.

This interview had consisted of series of questions (cited in: Appendix 3) with the theme of general enquiry into biometric development at Sagem [The Case Study]. Following the pilot, a number of observations were made and conclusions drawn in preparation for the primary investigation. The interview had ascertained the types of technology developed by Sagem, resulting in the decision to limit the investigation to fingerprint scanning and facial recognition systems for access control. The main themes had rested with social, legal and ethical perceptions of supply, acquisition, implementation and usage. It was important to gather common problems and methods by which practical issues could be addressed. It was also considered appropriate to enquire about European Government initiatives to develop and recognise the global
standard for commercial applications (ISO/IEC TR 24714-1-2008) relating to Information Technology and Biometrics.

The responses to interview questions were candid and informative but revealed some refinements necessary for subsequent interviews. This was to ensure that they most closely followed the path developed for investigation within the research objectives. The structure of the pilot interview was subsequently refined to provide clear boundaries for discussion. The second question made specific reference to what was considered to be the landmark date, and the critical security issue posed by the events of September 11th 2001. This refinement was important in providing participants with an historical landmark or boundary from which issues of personal identity and security had perhaps had the greatest cause to increase in significance.

The main refinement at this stage referred to the need to apply the theoretical perspective established within the study. The interview was altered to introduce questions relating to consultation and the application of institutional models. This provided opportunities for the theoretical framework to be supported or rejected within the empirical study. This refinement provided opportunities for insight into social, legal and ethical perceptions of biometrics, with a qualitative assessment of its effects on stakeholders and subjects.

4.9 Chapter Summary and Conclusions

The aim of the research path has been: To investigate the implementation of biometric technology for access control to specific workplace environments in order to develop a series of Recommendations for “Best Practice” in maximising social, legal and ethical acceptance. This research has focused on the United Kingdom but further research may be conducted in the future, to identify partnerships with the European Union and ultimately wider global applications. In this respect, questions relating to the ISO/IEC TR 24714-1-2008 have been further refined with “prompt” questions and subsequent enquiry into knowledge and usability as perceived by subsequent interview
participants. Again the aim is to build a theory based on informed knowledge of the scope available for this technology currently and in the foreseeable future.

The pilot exercise has revealed a balance in the biometric technologies chosen for this investigation, involving fingerprint scanning and facial recognition, being more firmly established and perceived (in some cases) as more reliable. In contrast, iris scanning, voice recognition and the developing technologies continue to require specific consideration for societal acceptance.

The experienced, professional assessment expressed by the research participant during the pilot, has gone some way to justifying and confirming the choice of biometric samples for this investigation, in the light of an expanding range of sophistication in biometric technology. Furthermore, the considered view of the participant in the need for practical responses to be made to organisational standards specifically (if not exclusively) within the United Kingdom, led to the representative sample being confirmed.

The pilot study has led to a three-way approach to the primary investigation, in which semi-structured interview questions have been addressed to management and the workforce to ascertain policies and standards from both management and workforce within the organisations in question. This has resulted in the development of a series of Recommendations for maximising social, legal and ethical acceptance of biometric technology for access control in workplace environments.
Chapter Five

Identification and Presentation of Current Practice
5.1 Introduction

This chapter identifies the case study participants selected for the investigation. It outlines the rationale and background of each case and discusses the processes (in terms of location, timing, management and procedures) for interviewing management and workplace participants. The primary consideration for identifying a suitable sample is based on the extent to which selected organisations are representative of the topic under investigation.

Burns and Burns (2008: 198) defined a representative sample as: "Any part or cross-section of a defined population which is selected on a probability basis and from which information can be obtained...or predictions made about the entire population."

This rubric has been applied in selecting an appropriate sample size for the current investigation. The decision is based on the assertions of Silverman (2005: 36) referring to the link between sampling and validity in raising questions about social practices that are possible or practical, as opposed to attempting to provide "categorical truths." The current sample has been selected by balancing a representative number of organisations with a manageable sample for investigation, to arrive at objectively defensible possibilities for social, legal and ethical perceptions of this technology.

5.2 The Case Study Selection Process

The four organisations chosen for investigation are based in the United Kingdom, (represented by Case Studies A to D). They include an educational establishment catering for one hundred percent overseas students, representation from Local Government, a Public Communications industry and a representative of the Aviation industry. All four organisations are involved in the implementation of biometric and other access control strategies.

An embedded format is used in the investigation (Yin, 2003). This involves analyses of various discourses from interviews with representatives of management and workforce within the selected organisations (Silverman, 2007). The interviews focus on a series of biographies. Participants describe their world, casting aside any attempt to build "true pictures" but concentrating on the relationship between interviewer and interviewee in
generating plausible accounts (Silverman, 2007:154).

The constructionist approach is undertaken to ensure accuracy of interpretation, using a process of content analysis. This has resulted in triangulation of data collected by interview producing a more reliable method for verification, using observational methods (Ticehurst and Veal, 2000). This approach addresses the conventional risks imposed to validity, reliability and generalisation traditionally associated with the collection of primary data. It does so by recognising that validity may be compromised by the meaning of responses to interview questions. The process of investigation responds to such risks by linking theoretical and applied research in establishing a series of objective assessments from management and workforce. This is achieved by the application of a conceptual framework combining the philosophy of Utilitarianism, the Hierarchy of Needs and the Psychological Contract.

5.3 The Interview Transcription and Editing Process

The rationale for the transcription process was based upon a systematic approach in which interview responses were read through, to identify patterns or themes common to respondents (Boyce, 2006). This process resulted in the emergence of a variety of themes capable of being grouped for subsequent presentation and analysis. Management and workforce perceptions were collated separately and separate groupings were identified for those who expressed favour in the provision of access control facilities, in contrast to those for whom the technology held little or no social, legal or ethical significance.

Responses from this process were subsequently collated and distributed to interviewees representing both management and workforce stakeholders from all four case studies. The final selection of respondents towards the compilation of “best practice” indicators (from Cases A and C) emerged from the transcription of responses from stakeholders represented by management (policy makers) and workforce members (subjected to various levels of acceptance towards biometric access control technology). The ultimate decision as to the appropriately selected sample for transcription, arose from a series of indicators of common feedback emerging from a representative sample of stakeholders.
5.4 Case Study A

The first organisation under investigation is Case Study A (a higher education institution) based in central London. The college is set up to provide formal education for international students. It provides a wide spectrum of educational programmes, from Certificates to Master's and Doctoral degrees, spanning a variety of subject areas. The college works in partnership with both public and private sectors within the United Kingdom.

Its mission statement is cited as:

"....a mission to provide affordable, excellent academic and professional education underpinned by research, scholarship and creative work and values," supplemented by the following objective: "...an international educational institution emphasising concepts of access to education, respect for individual students, facilitation of the learning experience via quality critical thinking and academic rigour to provide quality, affordable education for students from varying backgrounds, experiences and ages / citizenships who can flourish as scholars with direct personal and intellectual proximity with carefully selected facilities of distinguished professors.....".

This case focuses on the international nature of student provision. It recognises that visa extension may be made available for further study at the college. This follows student submission of passports to the Admissions Officer who has authority to make applications for visa extensions on students’ behalf, in strict compliance with United Kingdom Home Office Regulations.

In parallel with other similar educational establishments, Case Study A complies with United Kingdom and European Union legislation. This spans the Human Rights Act 2000, the Freedom of Information Act 2000, the Data Protection Act 1998 and the Public Interest Disclosure Act 2010, together with those areas of legislation protecting rights to equality, consolidated within the Equality Act 2010. This legislation ensures that citizens in the United Kingdom enjoy confidentiality of all information obtained, together with respect for their personal lives, rights of expression and equality of treatment.
Elements of this legislation, specifically those associated with data protection, together with the College Code of Conduct for Students, are clearly communicated to all entrants upon enrolment. Positive reception of this documentation is taken to represent acceptance and agreement to the rules and regulations of Case Study A.

5.4.1 Semi-Structured Interview with Management

A semi-structured interview was conducted with the College President between 13.30-14.30 on May 17th 2010, during which the interview questions (cited in Appendix 3) were introduced to the respondent and considered in systematic progression.

In response to initial questions about the introduction of biometric access control technology into the organisation, the respondent explained that the system has been in operation since 2009, in compliance with requirements of the United Kingdom Border Agency. He explained that whilst a biometric system was not compulsory, college management had chosen to undertake an in-depth study of the security systems available. The chosen system was considered to be the best on the market at that time to fulfil the three-way student, college and Border Agency requirements. He suggested that a robust security system was compulsory at this private college providing admission into the United Kingdom for 100% overseas students,

The respondent explained that the system works with between 300-400 (full-time and part-time) students on under-graduate and post-graduate Business Administration programmes. Prior to the introduction of this system, the college had used attendance sheets as a means of monitoring student absence, with sheets being signed and maintained in hard copy format.

The current biometric system uses single modal and single factor technology. It recognises the risk of system failure, in which case return to the hard copy signing would be the current contingency. The respondent acknowledged however, that, to date, system failure had not been experienced so the effects of potential vulnerabilities have not been tested or assessed.
The system uses fingerprint scanning technology to monitor and manage staff and students’ attendance. The respondent revealed an improvement in attendance rates for both categories of user since its inception. He explained that at both planning and procurement stages, consultation was undertaken with system suppliers to assess vulnerabilities relating to reliability, experience and perceptions of safe usage. He commented that there had been no formal organisational policy applied by the college beyond the criteria of “need.” Individual approaches were taken to informing subsequent users that concurrent systems of signage and fingerprint scanning would be in operation in the first instance. This provided the opportunity to practically compare the two systems and to assess their respective social, legal and ethical impacts.

The respondent acknowledged a variety of initial concerns arising from the implementation of this technology. He suggested that these concerns had been responded to with clear organisational strategies; explaining the rationale and potential effects of the biometric system to staff and students. There were assurances that the chosen system did not store personal data but converted scanned data into binary code. These assurances lead to the balance of security and anonymity considered by the college to be necessary for access control management.

Beyond concerns for ensuring privacy and respect for personal data collection processes, no further issues were reported from college personnel. This led to a general perception of satisfaction with the access control system with recognition of its potential to enhance security. This was reinforced by management pledges to comply with Data Protection legislation in ensuring the fair and lawful management of personal data extracted from the biometric system. Beyond the Data Protection Act 1998 and associated legislation, however, there was no evidence of general appreciation of European Standards and projects dealing with the social, legal and ethical management of this technology for access control.

It was suggested that logistically, the system assumes an 80% level of student attendance, as set out by the United Kingdom Border Agency. This regulation had been rolled out across student / staff access control management, applying to 14
administrative staff and 26 academic members of staff throughout the college. Combinations of experiences were reported: from 100% staff acceptance to 60% student dissatisfaction at some time since its introduction. Students reported resistance to the regulation of attendance, whilst they expressed no resistance to the potential effect of this technology upon personal rights and freedoms.

It was reported that Management has responded to student concerns as they have arisen, using a combination of explanation and negotiation. It was stressed however, that there is little practical room for manoeuvre where Government edict applies. Despite this inertia, the respondent suggested that a structured procedure is adopted to ensure consistency in response and feedback to all recipients. He pointed to regular dialogue having been undertaken between college managers and welfare officers.

In response to reported resistance arising from the need to apply a time-lapse error facility, the respondent recognised that refinements of this nature had been necessary. Provision had been made for an average time-lapse of between 10-20 minutes each side of a registration period. This change had been put in place to overcome risks of back-log at times of heightened access to the building and its constituent parts.

The respondent also acknowledged the potential need for an individual approach to system management to deal with specific issues arising from the use of access control technology. He alluded to management discussions having taken place about acquiring a total biometric package with additional facilities. For the immediate future however, he expressed his intention to continue using the original college database with its general student profiles. He suggested that this continued to provide logistical security in holding and storing personal information across a variety of systems. He recognised, however, that this approach may be treated with scepticism with its perception of data being available in a disparate way, presenting risks of mismanagement and misuse.

On reflection of future strategies for implementing biometric access control, the respondent reported no immediate plans to change procedures but he acknowledged that
opportunities may arise to roll out an integrated system in time. He stated that this would only arise however, if it were considered beneficial to the efficient running of the college. It would also have to balance the needs of the United Kingdom Border Agency with those of staff and students exposed to this access control technology.

5.4.2 Semi-Structured Interviews with Workplace Participants

Four on-line interviews were conducted between 18th and the 26th November 2010. They involved a sample of participants from the MBA Course Administrator, a Lecturer / Ed Excel Programme Co-ordinator, the MBA Course Director and an Assistant Office Administrator.

The interviews followed the interview schedule (cited in Appendix 4) beginning with a question relating to the background of security roles implemented within the college. Responses to this question varied, from a perception that there was no security within the organisation, to a detailed explanation of the implementation of its security measures. The latter response was perceived as having stemmed from social insecurity arising from the terrorist attacks on September 11th 2001. Another perception of the security roles within the organisation was linked to staff security checking. This was considered to be necessary to verify employment application information in an environment of trust, where the assessment of legal status within employment is recognised as being of primary importance.

The interview progressed to an assessment of access control measures since the terrorist events of September 11th 2001. Responses to this question ranged from a perception of security having been tightened across learning institutions but there was also a perception that the scale of large institutions prevents practical vetting of all those eligible to gain access and egress. Specific concern was raised about the potential for biometric systems to have a detrimental effect on attendance with negative implications for the overall educational experience. But, from a wider perspective, respondents appeared to appreciate the role of security controls in safeguarding information systems. They acknowledged the role of access control systems in managing sensitive data and thereby protecting its privacy and confidentiality.
The access control systems used within the organisation were cited with reference to a variety of applications. They ranged from the Synel biometric scan facility to coded locks and biometric access control using fingerprint scanning. This technology was cited largely in door access control systems, used also for purposes of attendance vetting. September 2009 was cited as the date of system roll-out and implementation. In the case of employees joining the organisation after that time, the existence, nature and effect of the system had been identified by management at the inception of employment. All participants acknowledged organisational strategies for the implementation of the system, with the majority expressing general satisfaction with verbal notification procedures.

Conversely, there was evidence of a lack of opportunity presented to the workforce for raising objections to this technology. On the question of whether objection would have been raised had the opportunity arisen, however, the majority of respondents indicated that they would not have done so. Only one respondent suggested that objection may be raised but they were not specific about how this would have been undertaken.

Having been asked to reflect on the reasons for raising or choosing not to raise objections, responses ranged from an appreciation that security systems of this kind are perceived as assisting the effective role of management in ensuring security. At the other end of the scale, there was an indication of apathy that such systems did no more than record attendance at the institution. The view was expressed that the technology tended to have a disruptive impact, with large volumes of students having to queue for the biometric sign in. This was considered negatively in the light of the system having no control over their decision to leave immediately following registration.

On the question of the technical mode and biometric approach implemented within the organisation, responses ranged from a perception of multi-mode (relating to the time of day in which the system operated: morning and afternoon), to that of single-mode (illustrated by fingerprint scanning examples for attendance). Confusion was evident here irrespective of an explanation of the distinction between single and Multi-modal applications, cited in the interview as follows:
"Do you use a single-modal (e.g. fingerprint or other) or a multi-modal (e.g. fingerprint, facial recognition and voice) approach?"

On the question of the "factors" adopted for implementing this technology, there appeared to be further confusion. The responses ranged from fingerprints being cited as a factor, together with pin code, in response to the question: "Do you use a single (e.g. smart card) or multi-factor (e.g. smart card, pin code and fingerprint) approach?" But there was clarity in response to the question of having been denied access to the biometric system implemented in the organisation.

Reference was made to incidents of false negatives (that is, not being recognised despite using an authorised biometric indicator). The reasons provided for denial of access arose through the intermittent need for prints to be applied to the system manually by the System Administrator, through to the experience of biometric systems failing to recognise genuine prints.

On the question of potential social, legal and / or ethical concerns arising from the implementation of biometrics, two participants cited possible legal and ethical issues but there was no expression of social concern. The legal concern for security was alluded to but not expanded upon. The perceived ethical impact arose from the necessity to register student attendance in an environment where attendance was not compulsory within the regulations, especially in the case of all students having attained the age of majority.

The nature of the institution and its association with overseas students specified from the outset that, in order for visas to remain operational, students must attain a minimum of 60% attendance. In assessing the value of the biometric system, however, a number of respondents perceived the potential for greater accuracy in the assessment of attendance when students' names were called from a role call in real time. It was suggested that this would provide staff with opportunities to observe any attempt by students to leave classes later in the day. Further concern was expressed that there was a danger of the system recording students' attendance over a limited period each day.
(both morning and afternoon) irrespective of those students having engaged in any activity other than the requirement to attend for study.

The interview progressed to assess the respondents’ knowledge of the current legislation protecting personal data and human rights. There was an equal split between participants having an appreciation of the legislation relating to the Data Protection Act 1998, and those with no knowledge of this or any associated legislation. Only one of the two respondents cited an appreciation of the law in this area, indicating that the legislation was brought to their attention at the time the organisation introduced the biometric system for access control.

On the wider question of whether the organisation had introduced participants to associated Standards and European-funded projects there was no apparent knowledge in any of these areas. However, all participants agreed that in their experience of biometric technology, no further measures were necessary to reduce concerns about the existence or effects of this technology. This suggested that there were no specific concerns in need of immediate response at that time. On the ultimate question of opinions or concerns to report at the introduction of this technology, participants suggested that the lack of concerns at this stage arose from its relative infancy within the organisation.

5.5 Case Study B

The second institution under investigation was representative of Local Government. The National Assembly for Wales Commission (provided for by the Government of Wales Act 2006) has responsibility for providing property, staff and services for the Assembly. The Commission is supported by staff in a series of Corporate Units.

The National Assembly for Wales has powers to legislate, creating a separate Welsh Assembly Government together with a Corporate Body: the National Assembly for Wales Commission (Assembly Commission). This occupies multiple roles from the setting of strategic aims and objectives to considering performance, agreeing standards and values, reviewing change and encouraging enterprise and innovation for the National Assembly. (www.assemblywales.org/)
Chief among the roles of Assembly business include legal services, human resource and finance issues, information and communication technology and broadcasting services to the Assembly Commission, estates and facilities management. This extends to external communications and the provision of security (dealing with all aspects of building and physical security) including access control management, security of public policies and implementation strategies.

5.5.1 Semi-Structured Interview with Management

The interview was conducted between: 14.00-15.00 on May 19th 2010. It was explained that until 2007, the Departmental role of Security Officer was associated with other security personnel with responsibility for information security. It had been formed into a Departmental Security Unit, reflecting central security arrangements in Whitehall. Today every Government Department must have a Departmental Security Officer (DSO), responsible for ensuring that the Department in question (in this case the Welsh Assembly Government) complies with the standards of security set by Cabinet Office in Central Government.

All physical security issues reflect Cabinet Office and the Centre for National Infrastructure (CONI). The requirement for threat levels associated with United Kingdom Government sector emerge from Cabinet Office, with (in general) some provision for local security issues to be taken by the Departmental Security Officer (DSO). The Welsh Assembly Government follows Whitehall, with the Departmental Security Officer (DSO) representing the Permanent Secretary’s Security Adviser, conducting investigations as required.

Local security arrangements reflect the individual building types with each office having a risk assessment scoring (low, medium, high) allocating security levels for each risk. This reflects the specific issues relating to use by Ministers (ranging from restricted to top secret) with (in the latter case) the level of risk assessment being set at “high.”
The semi-structured interview began with a request for the respondent to reflect on his perception of access control security since the events of September 11th, 2001. He suggested that the dual theme of terrorism and security arose with increased awareness by senior management that terrorism methods have developed and become more sophisticated since those of the Irish Republican Army (IRA), to the widespread use of suicide related behaviour. Emphasis was placed on the terrorist threat associated with Wales, with warnings that the Principality should not be complacent about its position in the danger facing the United Kingdom as a whole.

The respondent highlighted the need for flexible approaches to the implementation and management of biometric technology. He acknowledged however, that economies of scale have prevented a wide-scale roll-out of this technology with swipe card and digital lock systems prevailing in some leasing areas of the building.

The primary technology referred to was the proximity card, using fingerprint scanning for databases linked to close circuit television (CCTV). There was emphasis on the need for clarity of use in which the current technology is used solely for security as opposed to engaging in “function creep” into the area of time and attendance monitoring. The respondent suggested that this had arisen from a pledge undertaken with union representatives at the time of introducing the access control system. He further suggested that this is an important area of regulation, for individuals to maintain trust and respect in the access control usage of working environments.

On the question of contingency for malfunction, the need to ensure consistency and sustainability in the system was emphasised. The importance of maintaining a reliable service record, with the use of back-up centres and networked systems was stressed, to ensure triangulation of approach. The respondent highlighted this as a vital component in cases of specific access to security sensitive areas in which health and safety requirements may necessitate fail-safe opening systems. This may be a legal requirement to comply with fire regulations and associated risks to health and welfare.
The respondent explained that the system has developed largely since 2007, from a stand-alone swipe-card facility to a networked proximity reader and card. Back-up centres have worked to develop a series of minor systems for triangulation towards enhancing social recognition of a reliable service.

At its inception in 2007, the technology spanned proximity card and fingerprint scan, but it has since developed into a stand-alone network. Strategies have been adopted over time to introduce these systems into the workplace. This has involved a consultation process in which senior management has communicated with regional offices. Emphasis has been placed on a cost-benefit analysis whilst consulting with trade union representatives, disability groups and corporate health and safety facilities. The analysis process involved initial pilots with subsequent testing and re-testing within Information Communication Technology (ICT) systems.

The primary considerations in this environment rest with the security perspective of Cabinet Office as opposed to individual organisational strategies. This specifies that standards cannot be blurred to provide detection with no logo or name applying to identification or verification. It is considered unacceptable for authentication to rest on a Post Office Box number.

The major social concerns identified related to the dedication of Data Protection regulation, with care necessary to avoid covert monitoring for time keeping. The respondent suggested that staff had been consistently consulted to clarify practical “needs based” systems. This “needs” based analysis was recognised by the respondent as being “variable” or flexible. This recognised that individual perceptions of social, legal and ethical acceptance must be practical but may naturally merge.

The respondent explained that individual social and political climates determine distinct levels of security, with an example provided by the presence of the 2010 Animal Rights extremist movement towards the introduction of a policy of badger culling in West Wales. This necessitated an appreciation of both legal and ethical risks
to security for those working in government departments, with social expectation of specific measures necessary to ensure greater security.

Despite an undisputed risk element, the vital nature of biometric technology was articulated by the respondent. He outlined the requirement to monitor biometric access control to maintain the health and safety of the individual and to ensure equality and diversity throughout the working environment. He pointed to the Data Protection, Health and Safety at Work and Disability Discrimination legislation being necessary to ensure the appropriate management of these systems.

In comparison to the previous empirical studies undertaken for this research in which there was evidence of little practical knowledge of European Standards applicable to biometric access control, this respondent suggested that these organisations recognised both their existence and salient implications, with (albeit) office-run schemes cited for securing systems. He also pointed to existence of the Security Environment Assessment Panel (SEAP) in which technical representatives conduct regular risk assessment exercises to evaluate the use and effect of biometric systems.

The respondent suggested that this central role may explain the highly positive responses subsequently gained by workplace members, arising largely from agencies using commercial systems. This was evident despite there being no set procedure for requesting feedback, other than that arising from email or face to face negotiation.

On the question of the perceived benefit of these systems and changes to implementation of access control, the respondent pointed to systems developed to provide future-proof solutions with intermittent upgrades having been subsequently purchased. This had led to the development of consistent platforms to address social perceptions of a “suitable” environment in which to introduce security critical technology. The respondent applied this to visitor management systems up to “restricted” level. He acknowledged however, that stronger security procedures, reaching “confidential” level, should only be applied by the Ministry of Defence together with Home and Cabinet Office.
5.5.2 Semi-structured Interviews with Workplace Participants

Four on-line interviews were conducted between October 4th and November 4th 2010. A range of people were consulted, from a Farming Policy Executive, to the Head of Estates, an Employment Conditions Manager and a General Office Manager.

The interviews began with a question about the background to security in the organisation. This was responded to with an indication of the devolved nature of the Welsh Assembly Government to its Security Division. Reference was also made to the presence of security personnel at most large sites. This recognised that its status as a Civil Service-based organisation, rendered compliance with Cabinet Office guidelines necessary.

The interviews gained an appreciation of the perception of workplace participants towards access control, since the events of September 11th 2001. The responses related to personal safety and security within individual office spaces but concerns were raised about the level of equivalent security throughout the organisation. Overall, there was consensus that security issues and associated strategies had been given greater priority since the events of September 11th 2001. Emphasis was placed on the security of individuals within the area of access control. The respondents suggested that security within this organisation is paramount, with a general perception of levels being higher than those prior to the events of September 11th 2001. Reference was made to all staff with access to Welsh Assembly Government premises and assets having to undergo security vetting prior to entering the building.

On the question of the types of access control systems being used, the respondents referred to photo-smart cards and parking permits for access to the premises and locality. Reference was made to airport-style monitoring by security guards with scanning equipment used to identify personal possessions and to eliminate security risks. Respondents reported the use of access control technology in a range of applications. They included applications to enable security barriers and individual room locking facilities ensuring access to authorised personnel. It was suggested that systems
were consistently introduced upon recruitment and subsequent induction prior to access being provided to secure locations.

Respondents also reported a number of strategies being used to introduce this technology to the workforce. They ranged from verbal and written notification to the presentation of specific policies but they indicated a variety of methods being employed. One of the respondents suggested that he had received more detailed information about this organisational policy than was suggested by the other three.

Furthermore, on the question of opportunity provided to object to the use of access control technology, one respondent pointed to opportunities of this nature arising from induction. There were no reported objections raised, however, largely due to perceptions that the maintenance of security could not be improved with any alternative process. There were also suggestions that the majority of respondents had been given no practical opportunity to raise objection. On the question of technical modes, all participants referred to the current use of smart card technology as opposed to the use of biometric applications. Reference was made to single factor applications in which photo/smart card technology was reported as being used for access control.

There were no reports of access having been denied to respondents through false negatives, in which access may be denied despite authorised data being presented for access to secure environments. The main social, legal and ethical concerns ranged from the perceived need to be vigilant with the security of personal swipe cards. Largely for reasons of perceived familiarity, the use of swipe cards as opposed to biometric access control measures appeared to temper personal experience of this technology.

There appeared to be little evidence of personal reflection on social, legal or ethical impacts of implementing biometric technology save to consider the practical impact of personal identification. All respondents reported awareness of the current United Kingdom based legislation in place to protect personal data and human rights. The Data Protection Act 1998 was cited as having the potential to regulate the
circulation of personal data in the public domain. However, none of the respondents reported Data Protection legislation having been brought to their attention at the time the organisation introduced the access control system to them. Questions relating to organisational circulation of specific Standards and European projects for the practical management of access control technology led to there being no evidence of knowledge in these areas.

In conclusion to the interviews, participants suggested that there was no specific opportunity or social inclination to raise objections about the use of access control technology. Their reasoning was based on security measures being compulsory and socially advantageous throughout the organisation. They also suggested that, given the status of the organisation as a Civil Service environment, this technology was increasingly recognised as an essential element in ensuring the consistent regulation of security for individuals employed therein.

5.6 Case Study C

The third institution under investigation is representative of the Public Communications industry. This organisation introduced one of the newest and most advanced data centres in the world. It incorporates all appropriate and current technologies, having been purpose built to support the full range of hosting and managed service options.

The site is estimated as having a hosting capacity of 12,000 servers, capable of supporting total hosting solutions. Power for the centre is provided by two diverse sources with five generators acting as back-up provision, to guarantee 100% power available for every server.

The Cardiff site offers a variety of security systems, from reinforced double walls and fences, to digital camera provision, intruder detection, vehicle recognition and biometric identification systems. The Centre offers a range of services from hosting internet servers to the provision of complete hosting and web hosting solutions. This covers aspects of website design and maintenance, server operating systems, firewall and network management, with State of the Art security and monitoring systems.
The Centre has a sophisticated security system, providing multi-layered mechanisms (both physical and logical). This is supported by a certificate of compliance with BS7799: Part 2: 2002 and compliance with Independently Audited National Approval Council for Security Systems. Staff have undergone security vetting to Her Majesty’s Government Security Clearance (HMG SC) level. Access to premises is controlled by trusted employees, through electronic pass cards combined with retinal scanner-based biometric access control systems.

5.6.1 Semi-Structured Interview with Management

The interview was conducted 13.00-14.00 on June 16th, 2010. The respondent began by explaining that the sensitive nature of the Data Centre has led to physical systems being necessary to ensure security. This is evident by the presence of cameras at specific locations and both internal and external fencing protecting security critical areas. He suggested however, that, despite the impact of the terrorist attack in September 2001, there have been no changes in organisational strategy. The rationale is that security has always been regarded as paramount due to the nature of work being undertaken. The primary tasks relate to the hosting of data and equipment for banks and building societies through to Government and Ministry of Defence (MOD) related material.

The choice of technology rests with iris scanning facilities, implemented ten years ago. The respondent explained that the building in question has existed for seven years, leading to total familiarity of established staff to biometric technology for workplace management. Prior to the implementation of a biometric system, the organisation used pass card for access control, with a stand-alone system to administer security, using programmable cards.

The current iris scanning system was chosen because it represented the most viable solution to suit the needs of the organisation and its workforce. The system focuses on the maintenance of a secure access control facility for workplace management for both long and short term requirements of the Data Centre. The technology is implemented within levels of security ranging from SC (Security Clearance) procedures to secure
access to higher security areas, to DV (Defence Vetting) for top secret Government level documentation and equipment.

The former vetting process checks individual workplace members against their national insurance numbers and analyses their financial records to risk assess levels of susceptibility to terrorist threats. The latter process extends vetting to family and friends associated with workplace, to achieve a wider perspective of potential security risks posed by third party associates.

The iris scanning system meets a suitable flexibility standard by providing a range of measures from secure to high or enhanced security levels. The system is capable of being adjusted to read a particular eye, with an integrated inaudible alarm activated in the case of an alternative eye being presented to the reader.

The system uses a single modal and multi-factor facility with a perception that the enhanced security facility embedded in the iris scanning system has resulted in there being no outright system failure experienced. The multi-factor facility however, provides a fail-safe application with the card access system forming the available fall-back position.

The respondent referred to the system and procedure being risk assessed by fortnightly reviews to analyse the practical issues relating to time lapse. It also assesses security levels of individual rooms and specific locations integrated with technology. The system is capable of discriminating between iris images presented at enrolment and those subsequently presented as a match, towards forming accurate identification and verification of the individual.

Whilst there is no strategic organisational policy for the application of this technology in an access control capacity, the respondent pointed to a series of consultations taking place. They occur during the interview process (at which time appropriate security levels are assessed) within each building and part thereof, balanced against the various job functions of individual candidates, towards compiling accurate levels for Security
Clearance and Defence Vetting. The respondent suggested that this approach precludes the need for prescriptive organisational policies. It focuses on the practical design and implementation of specific systems for discrete environments.

The respondent reflected on questions of social, legal and ethical perspectives, suggesting that social compliance stems from the increasing recognition of "need." This applies all areas of security, whilst legal parameters tend to focus on knowledge and practical compliance with the principles of the Data Protection Act 1998. Emphasis is also placed on subsequent strategies for deleting data upon the expiry of individual contracts of employment.

Procedurally, the respondent pointed to the system using copies of the iris enrolled and presented with the associated name. This procedure secures identity, authenticating the data with the use of a desk-bound reader connected to a database. The respondent suggested there was no evidence of ethical concern arising from central storage in this instance. He pointed to procedural emphasis being placed on the peace of mind element provided by this technology in workplaces in which the maintenance of security has a series of benefits. He made specific reference to the health and safety of the individual and the practical effect of eliminating opportunist theft of personal property and confidential information.

Whilst he recognised the importance of the Data Protection Act in this area, the respondent made reference to this organisation being the first to recognise and demonstrate compliance with the ISO27001 for the Accreditation of Data Centre Standards with its universal recognition, where access security standards are audited by Lloyds of London.

Beyond nomination within the European Union, the respondent did not recognise other European policies and funded projects relating to the management of this technology. He suggested that the organisational approach was to focus on in-house regulation and compliance. He pointed to this strategy having been proven to be successful with a one hundred percent positive response from workplace members who appear to
acknowledge the need for privacy within these systems, ranking them above specific ethical constraints. The respondent further stated that this positivity in response is tested with quarterly security perception and enhancement meetings with representative groups. This has resulted in no adverse perceptions having been reported to line management to date.

With the benefit of wide-ranging organisational experience in implementing biometric security system, this management respondent reported purely positive perceptions. He suggested therefore that there were no planned changes beyond the application of new levels of software and the installation of new hardware to maintain efficiency. He considered that these procedures would focus on strategies for technology refresh as opposed to replacement.

5.6.2 Semi-Structured Interviews with Workplace Participants
Semi-structured interviews were conducted electronically from September 2010 to January 2011, with six respondents, representing members of the workforce within the organisation.

In response to the question of familiarity with access control systems, respondents reported experience in using iris and retina scanning technology together with electronic proximity cards. These systems were being used to maintain access control to secure data hall, office and building environments, for the requirements of individual employment roles. The respondents explained that the application of this technology had been introduced to them at the beginning of their employment. The timescales ranged from employment commencing in 1990 to a respondent having commenced employment in 2008.

On the question of organisational strategies used to introduce the systems to individuals, responses ranged from the use of one-to-one communication to briefings being provided by on-site security staff. The respondents also referred to written communication in which information leaflets were circulated to specific staff. One of the respondents
referred to a detailed security clearance form having been provided by line management with a request for completion and submission to Central Government.

There was no reference to organisational consultation above and beyond the use of verbal notification, but three of the six respondents in the sample, reported the use of organisational policies. One respondent suggested that the application of this policy had been clarified with her before her access to the building in September 2008.

Four of the six respondents indicated that they had not been provided with an opportunity to raise any objection to the application of the access control system

The two remaining respondents suggested that their acceptance or rejection of the system had been ascertained at the beginning of their employment, during verbal communication between themselves and Line Management. In both cases, where opportunities had been provided to raise objections about the use of this technology within the workplace; respondents reported that they chose not to do so.

In the remaining four cases, despite not having been presented with opportunities to raise objection, all the respondents indicated that they would not have objected. Their rationale was based on the need to implement access control systems within their workplaces. Only one of these respondents, whilst confirming that she would not have raised an objection to the system being implemented, suggested that she may have done so had she felt that there was no justification in implementing the system in question.

The respondents justified their decisions to accept the implementation and use of access control systems in their working environments with a variety of responses. They ranged from having researched the issue of safety and security in access control to having a clear understanding of its application in maintaining office security and protecting sensitive data in a non-intrusive way. This was supported with an assessment of the relative security of biometric access control systems as opposed to the use of swipe card technology. It was recognised that in the former case, the biometric trait cannot be lost or stolen, whereas in the latter, swipe cards are susceptible to misappropriation.
This was supported further with a perception that the use of biometric technology for access control would provide a positive perspective for existing and prospective customers. It would assist in their expectation of protection for business critical data within the organisation. There was also an assertion that the use of (in this case) iris or retina scanning did not represent an invasion of privacy or personal security.

Conversely, whilst agreeing that this technology represents a useful tool in maintaining security in specific areas, one respondent suggested that if the system were to be used in a more diverse way (for example, in monitoring workforce attendance) she would consider this to be an abuse of power. In expressing this view, she referred to the potential for biometric systems to represent “Big Brother” in their application to access control management. She conceded however that the application of biometric technology in this environment had been universally accepted as representing secure authentication for access control to safety critical data.

On the question of whether this application had ever resulted in denial of access arising from false negative responses to otherwise authorised members of the workforce, two respondents reported that they had experienced this. In each case, however, the respondents suggested that an acceptable solution had been found to secure access following engagement with the central (on-site) security system.

In cases in which scanning equipment intermittently failed to recognise respondents due to poor background lighting, a resolution was reported by the adjustment of scanner angles or the use of re-scanning. Whilst a solution was found by these procedures, the respondent alluded to having in some instances, to crouch or to stand on tip-toe, in order to gain appropriate recognition and security clearance.

Having considered the practical issues of implementing access control systems within the organisation, the interview proceeded to focus on issues of social, legal and ethical influences aligned to the application of biometric technology in this workplace. The social perceptions and concerns expressed ranged from security systems leading to guests at the organisation having to be chaperoned, with perceived constraints on the
mobility of personnel within the buildings. There were also concerns about access to and the security of data retained at the organisation. In addition, issues were raised about perceived risks associated with the potential to track and copy personal data acquired and stored within the organisation.

From a broader social perspective, a respondent reported her resistance to the more widespread use of biometric technology. She cited its comparative expense and her perception of the risks associated with this technology outweighing its benefits. Justification for this statement stemmed from a perception that in a relatively short space of time, criminal elements would find a means of falsifying identities and gaining illegal access to personal data. This respondent further considered the potential for such systems to become exploitative, in what she considered to be an increasingly authoritarian and governmental regime.

On balance, however, she recognised the relative benefit of this technology in its potential to restrict access to high security areas. But she considered that the use of biometric scanning of irises or fingerprints as being excessive for mere access to public places within the organisation. This respondent suggested that identification cards would be a more proportionate application in this case, but she alluded to the use of biometric access control technology in maintaining personal records and in the management of finances.

The legal concerns ranged from issues of data protection, considering who access to the information has recorded by biometric systems and where these details were kept. They also considered issues associated with justification for the retention of data. These concerns were tempered however, with reference to training in data protection legislation within the organisation, and the recognition that appeals could be made to challenge any suggestion of faulty evidence being generated by this data. The respondent further suggested that if biometric technology is to be more widely relied on, the whole issue of legal identity and its protection should be reinforced with further legislative provision.
The ethical considerations ranged from suggestions that organisations may use biometric access control technology to track the movements of employees. They also considered the perception of opportunities being provided to discriminate against minority groups in employment. Specific reference was made, in this context, to the potential difficulty presented by retina scanning towards members of the workforce who are blind or visually impaired. It was suggested that this may lead to appropriate contingencies having to be found to ensure consistency of application and equality of treatment.

In combining previous concerns raised by individual respondents, one respondent recorded a collective ethical concern, in suggesting that a regime in which organisations may have the potential to monitor individual activities, is morally wrong. In expressing this view, she raised two major arguments. Firstly, she suggested that technology that works effectively may be used as an instrument of oppression and exploitation. Secondly, she suggested that its vulnerability to being “duped” can lead to similar exploitation on a smaller scale; leading her to conclude that the application of biometric technology in access control environments of this kind, may be considered to be ethically unjust.

Having pursued issues of social, legal and ethical concern raised by respondents, the interview questions proceeded to link practical perceptions with an appreciation of European funded projects for access control within the United Kingdom. Whilst avoiding any suggestion that this should represent an exhaustive list, this question cited a number of examples of such projects. They ranged from ISO/IEC TR 27414-1-2008 – Biometrics, Jurisdictional and Societal Considerations for Commercial Applications and Design of Biometric Systems; EnCore (Ensuring Consent and Revocation) to PVNets (Privacy and Value Networks), VOME (Visualisation of Other Methods of Protection) and RISE (International Platform devoted to the Ethics of Biometric and Security Issues). This resulted in no respondents having reported knowledge or recognition any of these projects. The previous question led to the general question of respondents having suggestions for any further practical measures being
required to reduce the social, legal and ethical concerns cited in response to questions raised in this interview.

One response was made to this question, specifying the need for the organisation to clarify the implementation and application of the biometric system used. This was compared to the current procedure in which workforce members were perceived as being forced to ask specific questions about the practical applications of the system and its effects. This respondent recognised that questions were addressed by Line Management when they were raised but expressed concern about the possible long-term health implications of scanning technology being associated with facial features.

The final question focused on requesting remaining opinions and perceptions from respondents about the use of biometric access control systems within the organisation. This led to responses ranging from the need to ensure that access is appropriately controlled rather than utilised in routine and general applications. This was balanced by a perception that access control technology represents a sensible additional layer of security for sensitive areas of the building, and a perception that its application introduces discipline into the workplace. The use of identification cards was provided as a more rudimentary requirement for the sustainability of security, emphasizing the link between monitoring security standards and protecting the interests of customers and associates.

Despite there being a series of positive perceptions however, the respondent suggested that biometric access control technology should satisfy assurances of safe data management in which rights to informed consent in the acquisition, maintenance and storage of personal data is respected. In summary, this respondent clarified his overall support for the application of this access control technology in the workplace, subject to assurances that its speed of implementation does not compromise the consistency of its performance or its accuracy at point of output.
5.7 Case Study D

The fourth institution having been investigated is an International Airport, offering flights to both domestic and international destinations. In addition to aviation, the company also provides a variety of advertising solutions, through the use of light boxes, promotional areas, sponsorship and custom-built displays.

The airport is served by scheduled, low-fare and charter carriers with an estimated 75% of passengers reported as flying on charter services and 25% on scheduled services. Carrier organisations operating from the airport include Thomsonfly, MyTravel, KLM and bmibaby. It also supports corporate and general private jet charter for individual aviation use.

For development purposes both present and future, the company announced a £100 million development strategy in 2006 (completed in 2010). This investment plan anticipated a return investment of an estimated income of 400% passengers visiting the airport, forecasting an increase in its passenger travel capacity to 8 million by 2030.

5.7.1 Semi-Structured Interview with Management

The interview was conducted 10.00-11.00 on August 6th, 2010. At the beginning of the interview the respondent revealed that the airport is not currently using biometric technology for access control. The semi-structured interview focused on questions relating to management approaches to access control for workplace management and perceptions of biometric technology for this purpose, contained in questions 1, 11,13,14,16 and 26 (cited in Appendix 3).

The respondent reported the application of set standards towards this access control environment via the National Aviation Security Policy (NASP) applying uniform regulations across all United Kingdom based airports. He explained that the regulations apply to magnetic code access control for discrete zones, as required.

Management suggested that the United Kingdom airport security system is considered particularly strong in comparison with a number of European airports. Reference was
made to relatively recent terrorist incidents involving Paris and Amsterdam airports (in 2001 and 2009 respectively). In the first instance, the shoe bomber’s attempt to sabotage Flight 63 (from Paris to Miami) and in the second instance, a similar attempt aboard Northwest Airlines (Flight 253) from Amsterdam to Detroit Metropolitan Wayne County Airport in Michigan, United States. Whilst terrorist attempts were averted, the terrorists had succeeded in boarding the aircrafts in both cases. This compares with the attempt, for example on Glasgow airport in November 2010, where a security alert had arisen upon the apprehension of a suspicious package in the security area at departures (whilst proving to be of no security risk) had averted potential terrorist activity on board the plane.

Despite the recognition of coherent Government and internal regulation at United Kingdom airports, the respondent raised concern for the need to avoid social perception of an “inevitable threat”. In particular, the Department for Transport’s liquids policy risks creating a new fear level with the inevitability of producing detrimental effects on the social state of mind. In this respect, he suggested that, whilst the United Kingdom Government must be seen to positively assess and respond to risks of terrorist activity, this should be finely balanced with the recognition that any perception of fostering a “siege state” would be detrimental to United Kingdom society as a whole.

He further considered that, perhaps in partial response to the risk identified above, the Coalition Government expressed a preference to return to intelligence based access control as opposed to more intrusive strategies. The respondent recognised however, that research remains in this area towards assessing passenger safety and the potential role of biometric security, recently illustrated with the partial roll-out of body scanning equipment at Heathrow and Manchester airports.

The respondent in this study foresaw social reluctance to using body scanning equipment, having clarified that the airport in the case study had not implemented this technology to date. He expressed concern for potential social intrusion and individual perception of the surveillance state. He made reference to established Government edicts towards criminal records checks for airport staff in maintaining passenger
security; emphasising his view that this policy does not guarantee the prevention of fraudulent passport applications. Rather, he stressed that authenticity of captured images for identification are only as accurate as those stored on driving licences or other traditional areas of image recognition.

With reference to the decision of this organisation to use magnetic strip technology for their access control management, the respondent referred to contingency policies for fail safe systems being implemented using human recognition of image, supported with human authority to access specific zones and associated codes. He considered that contingency measures of this kind represent as accurate an approach to system failure as could be applied to any other access control strategy.

He suggested that biometric technology, using images and fingerprints linked to scanner points, would provide additional information. Conversely, he suggested that the nature of this organisation renders it unlikely to apply a unilateral approach to access control. The rationale here rests with the status of this organisation within the broader United Kingdom landscape, necessitating compliance with national standards.

From a broader United Kingdom perspective, the respondent maintained that biometric technology is associated with complexity and cost issues. He referred to the social and ethical negativity traditionally associated with public scepticism towards personal information being stored on databases, and its connotation with "Big Brother." He also acknowledged social perceptions of excessive Government intervention into everyday social life. In doing so however, he alluded to the comparison between perceptions of the United Kingdom and Spain. In the latter, no such widespread social resistance applies in an environment in which chipped passports have represented the norm since August 2006. In contrast, the respondent suggested photograph and fingerprint biometrics are likely to be the most socially acceptable in the United Kingdom, having limited association with social intrusion. In comparison, iris and retina scanning is traditionally associated with greater personal intrusion, complexity and excessive cost. On the wider question of social advantages of biometric technology irrespective of form, the respondent suggested that this technology will never be considered to be
100% foolproof. He pointed to evidence of social perception in this area in relation to the introduction of body scanning equipment at airports. Here social resistance has been evident irrespective of publicity attempting to balance this technology with security risks. The respondent suggested however, that social perceptions of this kind may be difficult to explain in the long-term. He referred to the United Kingdom Airport Security policy, recognised to offer an almost 100% safety record balanced against security risks associated with tube trains and buses since the terrorist attack on London in July 2005. In this respect, the respondent expressed difficulty in justifying the singling out of aviation for security measures over and above those applied to more conventional forms of transport.

In practical terms, the respondent suggested that aviation procedures to adopt biometric technology as a primary factor are only likely to emerge on a national scale if legislation is implemented to regulate this. In the absence of Government edict, he suggested that trade union resistance in the aviation industry has traditionally assimilated the introduction of biometric access control as a method for employers to justify exercising dominance over their employees. He suggested that this issue had been recently debated in addressing the possibility of a research project conducted into the potential use of Radio Frequency Identification (RFID) for access control within the aviation industry. The chip would enable employees to be monitored at each location, but this led to ethical concerns being raised towards the risk of developing a Big Brother state. Despite this, he recognised that in the case of relatively minor aviation points of reference, where there were fewer points of intrusion into personal life, discussions towards the application of this technology may not pose insurmountable problems, given the relatively minor unionised nature of this industry.

The respondent stressed the need to sell the security risk strongly but he suggested that convention dictates that any such introduction would need primary consultation with Government. He recognised that the ensuing dictates would inevitably constrain employee rights. He cited an example of enforced strategy post September 11th 2001, when criminal records checks were strengthened resulting in some (previously spent) convictions becoming operational. This led to convictions that would otherwise have
presented no constraint on the individual employee being no longer legally acceptable for the provision of airside passes, following the Department of Transport Regulations 2002.

This strategy resulted in employee dismissals following Government edict, leading to those who had originally been considered competent workforce members being made unemployable based on what would, in other social settings, be considered spent convictions within the Rehabilitation of Offenders Act 1974.

The respondent suggested that pragmatic questions should be posed as to where the line should be drawn in determining whether an individual represents a security risk. He pointed to the primary objective of the aviation industry to encompass freedom and ease of movement. The respondent considered that the risk should perhaps be weighed against the economic pressure associated with the implementation of aviation.

On the question of the multi-cultural workforce, the respondent considered ethical implications stemming from potential religious objections. In this case, ethical concerns were expressed to be relatively low given the strong British employee base but it was recognised that this should be compared with other United Kingdom locations, specifically those in London and Birmingham. In these cases cultural diversity has the potential to result in religious objections to the effects of biometric technology being used for access control management of the workforce.

In general assessment of the likelihood of biometric technology being used within this environment in the future, the respondent suggested that the most favoured biometric applications would be fingerprint scanning and facial imaging, in the absence of financial support from Government to develop market and implement a variety of biometric modes.

In conclusion, the respondent stated that current financial responsibility for access control management is taken by airport and airline authorities within the United Kingdom. Operators have responsibility for funding security in the current absence of
legislation to pass costs on to customers. This is resulting in the aviation industry being reluctant to introduce biometric applications based on pre-judged social perceptions of risk.

The respondent stressed the primary role of economies of scale have led to pragmatic management perceptions that the terrorism threat in the United Kingdom should not be represented or perceived as having the capability to be solved by the wide-scale application of biometric technology for access control management. He suggested that the lesser security threat posed by what he considers to be a relentless, subjective Press (often responsible for making the news rather than simply reporting it), often leads to similar domestic and international security risks, but remain financially justified.

5.7.2 Semi-Structured Interviews with Workplace Participants
Following the interview with management at the airport, an arrangement was made to return to conduct interviews with members of the workforce. The original research plan had been to return in September 2010 but external circumstances, relating to the previous management regime, resulted in an alternative arrangement. Following a number of contacts, three from a possible five participants were secured but the original research plan to interview them in person was subsequently precluded by work pressures at the airport. This necessitated a change in strategy, leading to a series of three on-line interviews being conducted between October 2010 and February 2011. The airport staff ranged from a representative of ground staff to an administrator and a check-in operator at the airport.

The first on-line interview was conducted with a representative of ground staff working on a full-time (shift-rotation) basis. In response to the initial question relating to the type of access control system with which he was familiar, he referred to magnetic strip technology as having been the primary access control management application since he began employment at the airport in April 2007. He suggested that this technology is used in discrete zones, in which security measures are necessary on the ground, ranging from baggage handling and storage environments to specific security sensitive areas throughout the terminal building and its parameters.
The respondent recognised that the technology had been introduced to him at induction into employment in April 2007. He suggested however, that he had prior knowledge of similar security systems within other airports at which he had been employed within the United Kingdom, including Birmingham and Manchester Airports.

Whilst he reported that verbal and written communication had been provided at the beginning of his employment at this Airport, he stated that he had not been consulted about his previous knowledge of airport security technology nor had his opinion been sought about his perception of the current system. He recognised, however, that both induction and follow-up written documentation had explained the rationale and application of the current security system being implemented at the airport, albeit in prescribed form, rather than during any course of dialogue. Despite this, on the question of whether he would have provided constructive feedback or raised queries or objections about the current system, he said he would not have done so, citing reasons of perceived futility. Perhaps more specifically, he stated his reasoning as being based on his primary concern for personal safety together with that of airport personnel and passengers.

On the question of utilisation, the respondents were initially uncertain of the distinction between single and multi-modal applications. Upon clarification, the respondent indicated his appreciation of the concept of single modal applications, whilst utilising the magnetic strip technology. His response to incidents of denial of access referred to the perceived inconvenience of there being no contingency access provision when the card is not available. In other respects, he conceded that he had not experienced denial of access arising from a false negative, suggesting that, his experience of the current security provision is positive.

On the question of biometric technology being used for access control, whilst he alluded to not currently having experienced biometric access control provision, he suggested that he would have no initial concerns, be they social, legal or ethical. He explained that in his estimation, the need for security should be placed above personal issues and perceptions.
The interview proceeded to questions of familiarity with established standards and funded projects relating to the management of biometric technology. Whilst he suggested that none of the cited standards were familiar to him, he made reference to the existence of a national policy associated with airport access control. He acknowledged that he was unaware of the precise title of this policy, but appreciated that the nature of the policy is such that it must be implemented consistently throughout the United Kingdom.

This led to the question of whether more stringent security measures could be taken at the airport to further ensure the consistent management of security. In response to this, he suggested that research should be undertaken with a view to introducing a variety of technology to adapt to individual security environments. He stressed however, that he did not, at this stage, feel that any specific technology could be cited in the absence of further research into practical applications and budgetary commitments at the Airport.

On the final question of his general perceptions relating to the application of biometric access control technology, the respondent concluded that, in the absence of specific, fully-funded research, the current security facility using magnetic card technology appears to be as effective as any other, with similar budgetary constraints.

The second on-line interview was conducted with a member of administrative staff at the airport. The respondent began by explaining that she was a relatively new employee, having been employed at the airport for the previous six months.

On the question of familiarity with access control systems at the airport, she suggested that apart from having been introduced to the issue of security management in her training programme and having been referred to the National Aviation Security Policy implemented by the airport, she had very little knowledge of access control technology, beyond that of the magnetic card system operational at the airport. She explained that her current employment was her first experience of the aviation industry.

Before this, she had been employed in the retail industry, in which she had been introduced to the principles of security within Radio Frequency Identification, in its
application to various goods and services. In response to the question of the strategies adopted by this organisation to make her familiar with its security system, she expressed uncertainty as to whether there had been any verbal notification of the security policy within this environment. She recalled only verbal reference to the magnetic card at induction and in subsequent training sessions. She also referred to documentation having been provided at induction referring to the organisational (National) security policy being implemented at this Airport in conjunction with all other United Kingdom based airports.

The respondent was clear that no opportunity had been provided for her to object to the application of this technology and she further suggested that little explanation had been provided about its practical usage, other than that applicable to her specific role. Despite this, she suggested that she would probably choose to comply with any security system introduced to her at work. Her rationale for this was that she lacked the appropriate knowledge or experience to question organisational standards, specifically those associated with security.

On the question of usage from single or multi-modal perspectives, the respondent appeared to be uncertain of the distinction between the two applications, but, following clarification, she perceived the magnetic card system to be single modal.

In answer to the question of her experience of denial of access resulting from false negatives, she stated that she had, through her own fault, experienced instances in the past, albeit isolated events, in which access had been made impossible due to her card not being present at specific times. In reflecting on any practical concerns she had relating to the implementation of biometric applications for access control management, the respondent expressed her uncertainty as to the specific nature of this technology. In explanation, two examples of biometric technology were illustrated, relating to fingerprint scanning and facial recognition systems.

In response to these examples, the respondent suggested that, whilst there may be few social or legal concerns in the current environment of relative insecurity within both
personal and working lives, she was concerned about the risk of this technology falling into the hands of unscrupulous people, from employee and management perspectives. She focused concern on the propensity for such people to use biometric technology for unauthorised purposes, in perhaps gaining access to unauthorised and / or confidential data. Beyond that, however, she said that the development of this kind of technology is necessary in the current social climate where (in some respects) personal safety is increasingly recognised as having to override human rights to dignity.

The respondent said she had no recollection of the variety of European Security Standards and funded projects for biometric access control having been brought to her attention in her current employment, beyond having sight of the airport policy relating to security.

On the final question of personal concerns relating to the implementation of this technology for access control, the respondent suggested that her limited experience and knowledge in this area rendered her objective view prohibitively limited. With reference to the explanation of fingerprint scanning and facial recognition technology, she recognised however, that the development and application of these technologies is becoming increasingly necessary to secure both people and property within sensitive areas of society. But in doing so, she expressed concern for the way in which this technology is being managed, suggesting that perhaps it is only as useful as its management.

On overall reflection of her general perception of the implementation of biometric access control systems within the Airport, the respondent suggested that her judgement would remain reserved until there is clear evidence of the need for this technology. She further suggested that in the event of proven need, the technology should be accompanied by an objective, well-informed policy, communicated to all staff. She stressed that this strategy would alleviate suspicion and fear about the propensity for the technology to be abused by management and / or government influences beyond the control of those to whom it applies.
The third and final respondent engaging in the on-line interview was a Check-in Assistant employed at the airport. Whist alluding to the fact that the organisation did not currently use biometric technology for access control, he suggested that he had experience of the practical implementation of this technology within his previous employment. In this context, he had been introduced to electronic card control systems using iris scanning technology to facilitate physical access control in the late 1990s.

In respect of this previous system and the current magnetic card device, he explained that verbal notification had been introduced in both cases, using established organisational policies. He indicated that, in his previous place of employment, he had been trained in the use of the technology at the time that the organisation made verbal reference to its existence and implementation. This process of introduction and training had arisen during the induction phase of his employment.

On the question of having an opportunity to raise objections to the implementation of the current magnetic card system and previous biometric applications, the respondent suggested that this opportunity had not arisen. He specified however that the organisation had provided electronic feedback systems, allowing staff to raise concerns as they arose. He further suggested that the then organisational policy in existence, specified opportunities for workers to make recommendations for more effective use of this access control application.

Focusing on his previous experience of iris scanning for workplace access control, the respondent indicated that he had conducted research into the effects of this technology using the internet as a research tool, before having to comply with this access control system. He indicated that the results of his research had confirmed his lack of concern about the safety of iris scanning systems in particular and biometric technology in general. He further specified that he had no human rights-based objection to complying with the application of biometric access control for workplace management.

The respondent failed to respond to the question relating to the status of the access control method being used, either at his current place of employment or that in his
previous place of work. But, on the question of whether access to specific working environments had been denied in his experience due to the presentation of a false negative, he had not experienced this type of incident to date.

In response to the question of his perception of the reasons for general concerns relating to the implementation of biometric systems for access control, he suggested that in his relatively narrow experience of such systems, he had rarely witnessed general objection. He clarified however, that in cases where objection had been raised this had been solely associated with individual perceptions of medical risk arising from the implementation of iris scanning technology. This perception was qualified by there being no social, legal or ethical concerns either having been experienced by the respondent personally or witnessed within his fellow workers.

On the question of knowledge relating to Standards and European funded projects, the respondent indicated a general lack of awareness of these provisions to date. In assessment of his perception of biometric access control within his previous workplace, he suggested that hundreds of his colleagues had accepted this technology without question. He had witnessed only one objection; arising on medical grounds, associated with iris scanning technology. And, in final assessment of his perception of the current access control environment using magnetic strip technology, he confirmed that he had not witnessed any external pressure for revision of the system on grounds of health or for the preservation of general human rights.
5.8 Chapter Summary and Conclusions

This chapter has discussed the case study participants chosen for the primary investigation, identifying the semi-structured interview approach undertaken with management and members of the workforce, from Case Studies A to D.

Each of the cases has been selected following more widespread investigation into organisational perceptions of biometric technology used for access control purposes. Subsequent sample sizes were represented by academic texts considered to be manageable in addressing the ultimate aim of the investigation. The samples were further chosen to represent elements of United Kingdom-based Public and Private Sectors within disparate areas of potential biometric access control technologies from areas of Education, Government, Public Communications and the Aviation industry. This chapter has resulted in the presentation of a first-cut audit of initial feedback from research participants on questions of organisational perceptions and implementation of biometric access control from management and workforce perspectives.
Chapter Six

Analysis of Best Practice and Development of “Best Practice” Model
6.1 Introduction

This chapter undertakes an assessment of the general concept of "Best Practice" in developing a series of recommendations for implementing biometric access control procedures within the case studies under investigation. The process leads to a series of first cut suggestions being sent to a sample of respondents selected from Case Studies A and C for consideration, comment and assimilation of suggested "Best Practice."

6.2 Suggested "Best Practice" Model

Having undertaken a series of primary investigations into the application of biometric access control systems in a range of United Kingdom-based organisations, the current (practical) provision of security standards within the United Kingdom has been analysed. This analysis has been undertaken in conjunction with the practical application of a policy established in the United Kingdom since 1995 for the maintenance of information security management. This policy was introduced by the United Kingdom Government Department for Trade and Industry (DTI) and published by the British Standards Institute (BSI) as a formal strategy for the maintenance of "Best Practice" in information security management.

The initial title of the policy was BS7799, but following consultation between the United Kingdom Government and international standards bodies, it was revised and adopted by the International Organisation for Standardisation (ISO) in 2000. It then became ISO/IEC (International Electro-technical Commission) 17799: (27002) Information Technology – Code of Practice for Information Security Management (Saint-Germain, 2005: 61): (cited in: Figure 5)
Figure 5

Subsequent refinement of this Standard in June 2005 and July 2007 resulted in its incorporation into a series of standards, representing a methodical compliance framework. The Standard is currently entitled: ISO/IEC 27002 Information Technology – Security techniques – Code of Practice for Information Security Management. It contains twelve suggested information security controls (a sample of six of which have been applied in the current study).


(Extraction of six from twelve suggested information security controls)

1. Risk Assessment and relevant management;
2. Security Policy and management;
3. Human Resources Security – for employees joining, moving and leaving the organisation;
4. Physical and environmental security – protection of facilities;
5. Access Control – management of access rights to physical and technical applications; and

6.3 Application of Suggested Model to the Selected Samples

Whilst the process of investigating a best practice model had been reasonably unhindered within all four case studies, greater ease was experienced in gaining access to both management and workplace participants in two of the four cases involved in this study. There were a variety of practical, human resource reasons for the relative difficulty experienced in the research process at the government-based organisation and within the representative of the aviation industry. These issues had emerged primarily from the security critical nature and workload implications associated with these
organisations and the relative difficulty in gaining consistent access to critical personnel. There had also been an unexpected change of management in the aviation environment. This had resulted in logistical problems in maintaining personal contact with specific individuals with whom discussions had taken place at the beginning of the research process.

The procedural issues at these two organisations led to the decision to concentrate primary investigations within the two organisations with whom the initial process of empirical enquiry had resulted in fewer strategic issues. The rationale for this was based on the assertion of Silverman (2005: 36), in which he referred to the academic value of an attempt to raise questions about the social practices that are possible (or practical), as opposed to attempting to provide "categorical truths."

Based on this rationale, it was proposed to conduct in-depth studies with Case Studies A and C, where primary investigations had been conducted in a relatively consistent manner. In these cases there had been little or no change of management or interruption of procedures in conducting investigations. This led to email contact being made with previously contacted representatives of management at both organisations. The emails sought permission to send a series of (first-cut) "Best Practice" suggestions for biometric access control procedures to achieve social, legal and ethical acceptance, based on the responses gained from initial primary research conducted at these organisations.

Following consent from each of the selected organisations, a (first-cut) series of suggestions for "Best Practice" were compiled and sent, following which an electronic response from management and workforce members was awaited. It had been envisaged that the conclusions and recommendations arising from this (second) process of investigation would form a practical rubric for the social, legal and ethical application of biometric access control management. This "Best Practice Model" would be subsequently applied within all four sample case studies, in addition to its more widespread application to associated organisations within the United Kingdom.
6.4 Presentation and Analysis of feedback from representatives of Case Studies A and C

6.4.1 Background

Participants representing Case Studies A and C, were asked if they were prepared to be identified as having participated in this research process. They were subsequently sent consent forms to indicate their acceptance of this process but were informed that if they wished to remain anonymous, their decision would be fully respected. Both participants expressed wishes to remain anonymous leading to their being subsequently referred to as: Case Studies A and C.

6.4.2 Participant Responses and Analysis

Case Study A

In this case, there were twelve suggestions for “Best Practice” selected from first-cut responses of management and workforce representatives (cited in: Appendix 5). The first suggestion arose from management and workforce reporting that no current formal institutional policy had been adopted to implement signage and fingerprint scanning applications. The suggested policy referred to the need to introduce a security strategy and to confirm practical management procedures for its implementation.

The second point for suggested “Best Practice” related to there being institutional knowledge of domestic legislation but no evidence of knowledge of European regulations, Standards or funded projects for access control management. The suggestion for “Best Practice” here related to the perceived need for the college to introduce and implement information systems policies incorporating European Standards, laws and regulations, including reference to associated (funded) projects to secure consistent access control systems.

In response, the respondents considered this strategy to be optional only, citing the main concern of the college as applying to student attendance, for compulsory feedback to the
British Home Office. Whilst the respondents indicated that knowledge of additional legislation would be useful, they did not consider this to be a primary function of their access control system.

The third issue related to the management perception that Government edict in the control of secure access, rendered procedures for explanation and negotiation a secondary consideration. This led to a “Best Practice” suggestion involving the introduction of a human resources strategy, in which specific information would be provided to employees upon joining, moving within and leaving the institution. This suggestion was intended to highlight the extent of institutional control over access security management. The institutional response was measured, with partial agreement in relation to staff who are directly involved with access control management. There was a perception, however, that this level of human resources intervention would not be practical in areas where the control of access is compulsory for both staff and students.

The fourth point referred to management plans to introduce a total biometric package responding to concerns about the misuse of data. The “Best Practice” suggestion here referred to the institutional need for management to undertake a consistent risk assessment and response of the proposed procedure. This was ultimately received in a positive way with a statement indicating that the system had been implemented between the initial primary investigation and this subsequent receipt of a series of (first cut) suggestions for “Best Practice”.

On the question of management plans to introduce an integrated system for access control management in conjunction with Border Agency regulations, the respondents indicated that whilst they agreed that this strategy should be adopted, they alluded to there being no current plans to implement the system. This led to support being expressed towards the suggested practice of clarifying the current security policy established at the institution. Emphasis was placed on ensuring social, legal and ethical compliance for data security and integrity, with the implementation of (previously negotiated) practical management approaches.
Whilst the previous suggested strategy was wholly supported by the respondents, the following (sixth) selected response from the primary investigation indicated that student perceptions of the biometric access control system were largely negative, in response to attendance and the overall student experience. This led to a suggestion that *management should consult with students towards introducing a human resources security strategy, in which there would be consultation with and advice for those joining, moving within and leaving the institution*. This suggestion was partially supported by management, with respondents emphasising the need to maintain the message of compulsion whilst showing some tendency to dialogue (if not flexibility) in the management of and link between security and attendance.

The seventh issue, related to workforce suggestions that opportunities were not consistently presented to raise objections about the implementation of biometric technology within the institution. This led to the proposal again, that *human resources security policies should be available for those entering, moving within and leaving the institution*. Management responded negatively to this suggestion however, expressing the view that the relatively small size of the organisation rendered this type of strategy unnecessary.

Similarly, the eighth suggestion, that *management should implement clear security policies including reference to concise management methods*, received a negative response. Management justified the reported perception that no specific opportunity had been provided to raise objections about the implementation of access control technology. Its justification related to the relatively (small) size of the institution, rendering a large-scale strategy of this nature difficult to objectively defend.

In answer to the respondents’ suggestions that they have reasons for security systems clarified to them, the suggested “Best Practice” referred to *risk assessment and management to reveal access to relevant physical and technical applications*. This was partially accepted by the respondents, with emphasis on its application to staff at the institution as opposed to the larger student cohort.
In response to the micro-management of both false positive and negative applications, it was suggested that a combination of risk assessment and associated management of physical and environmental security should be accepted by all respondents, in order that all those with access rights at the institution, perceive the control facilities to be effective, efficient and reliable.

This issue of positive perception was further considered in response to the combination of social, legal and ethical concerns enunciated within the primary investigation, leading to a suggested practice of developing information security policies to incorporate Standards, laws and regulations. The respondents expressed agreement with this strategy acknowledging its necessity in implementing effective access control technology. These strategies were reported as being currently implemented (in part) within induction procedures and associated documentation.

The final issue related to the perceived uncertain extent of current knowledge within the institution relating to Data Protection and Human Rights legislation. This led to a suggestion of "Best Practice" whereby security policies should be consistently implemented by management so as to clarify Standards, laws and regulations for the protection of personal rights and freedoms. In response, it was indicated that Data Protection legislation is fully acknowledged and explained to access control participants upon their registration.

On the question of the application of more widespread legislation, the respondents suggested that the more diverse legal principles (associated with general Human Rights legislation) may be out of context with the legal regulation of personal data within the institution. This led to a generally expressed perception that Data Protection legislation, in its current application to the process of registration for secure access control, represents the necessary legal compliance with the Home Office edict applicable to access control management within the institution.
Case Study C

In this case there were ten suggestions for “Best Practice” selected from responses of management and workforce (cited in: Appendix 6). The first “Best Practice” suggestion arose from the management contention that there was no current formal policy for introducing biometric access control to the workforce, beyond a series of consultations during interview, in which security access levels are assessed. This led to a suggestion that the organisation undertake a review of access control management, focusing on physical and technical applications to ensure compliance with current Standards, laws and regulations.

Whilst the respondent recognised the importance of setting out consistent policies for access control management and reported general agreement that such policies should be considered, she tempered this with an explanation of the logic behind the current system. She explained that the current (formal) policy exists as a compulsory element of security control within the organisation, so that in a sense, the present practice of engaging in verbal communication with the workforce at interview and subsequent induction has traditionally been considered sufficient. She expressed the view however, that perhaps the extraction of salient parts of the ISO/IEC 27002 Standard should be incorporated into the staff handbook. This would formalise current security policies across the organisation, with this practice emerging consistently at local level and perhaps extending to national practice in time, supported with appropriate management-level consultation.

On a more specific point however, the respondent referred to security-related issues incorporated into individual contracts of employment. She suggested that workforce participants expressing concerns about security obligations should have consulted with their contracts of employment upon commencing employment at the organisation. She further suggested that, if they were not in agreement with any of the security-related obligations, they should not have agreed to their contracts. She emphasised that any subsequent attempt to flout contractual obligations, would be considered a breach of the contract of employment (service) in the case of employees and a-typical workers or the contract for services (in the case of contract workers and freelance personnel).

The second point for consideration of “Best Practice” arose from workforce representation that no organisational consultation had traditionally taken place between management and the
workforce relating to access control management other than verbal notification provided at the interview and subsequent induction process.

This led to a suggestion that "Best Practice" could be secured with a critical assessment by management of the current security policy at the organisation. It was suggested that management objectively assess the extent to which current communication practices with the workforce are considered “effective” from the perspectives of both management and workforce representatives.

There was general agreement expressed towards this suggestion but the respondent contended that the increasing significance of access control within the workplace and the need to ensure its appropriate management towards a socially acceptable policy, made consideration of one-to-one consultation within the workforce economically challenging. She suggested however, that the use of quantitative investigation, in the form of staff surveys, would more economically viable. She further suggested that empirical research and review of this nature may be linked with the current (mandatory) staff appraisal system undertaken within the department. She expressed favour with this practice, highlighting its potential for the effective assessment of workforce perceptions towards the management of access control and associated issues. This respondent cited the appraisal system as representing the most appropriate forum for obtaining staff feedback and carrying out management review towards designing a mutually acceptable system.

The third issue reflected upon workforce suggestions that any management plan to extend access control measures to monitor attendance, would be considered an abuse of power. This had been a strongly held view, expressed by more than one of the workforce participants. Whilst there had been no specific mention of the fear arising from potential “function-creep”, this had been implied, with reference to concerns that organisations may establish undue control over their workforces. In response to this, the suggestion for “Best Practice” related to management responsibility to ensure that the workforce is fully aware of organisational policies for access control management, specifically those associated with physical and environmental security.

On this point, the respondent expressed dissent, suggesting that any current pledge that access control management would remain static, could be misleading to the workforce and unduly restrictive towards a sustainable access control system for the future. She expressed the view that the current system is fully communicated to staff in terms of its implementation and subsequent effect on their day to day working practices. She suggested however, that the nature
of the organisation precluded any suggestion that more stringent policies would not be adopted for data control management in the future. She suggested that the need to use the system for purposes other than strict access control management would be difficult to defend however, given the emphasis on the ISO/IEC 27002 benchmarking practice at the organisation, focusing on data protection and the security of personal rights. She also pointed to the need for any such extension of practice to be preceded by union consultation, whereby representatives of the workforce would have opportunities to challenge management strategies towards using security systems to monitor the workforce. In conclusion to this point, the respondent suggested that the only (current) plausible link between access control management and workplace monitoring, would apply in cases where personnel had restricted access to data, necessitating an organisational inventory of access and egress in areas of specific sensitivity.

The next consideration referred to workforce concerns that scanning equipment used at the organisation had been subject to intermittent failure. This was reported to have led to organisational resolutions involving the adjustment of scanner angles, necessitating change of stance for access, leading to the perception that taller or shorter people may feel more or less intimidated by the prospect of false rejection. This was considered to be a potential social concern leading to evidence of some workforce resistance to this form of security technology, on grounds of perceived insufficient protection of human rights. The "Best Practice" approach in this instance, related to the suggestion that the organisation undertake a current risk assessment in areas of physical and environmental security.

The respondent reported having (to date) received no feedback either positive or negative, towards the operation of scanning equipment within the department. She expressed surprise at the workforce perception that scanning angles were adjusted but in doing so, she pledged to investigate this issue further. A potentially contentious issue arose at this point, in which the anonymous nature of participant response precluded any form of identification of workforce respondent. Whilst the management respondent did not expressly request identification, she suggested that it would be helpful to have some indication of the level of access associated with the workplace respondents in question. In the absence of this opportunity, she suggested that she would raise the issue in the staff bulletin provided to all staff on a monthly basis, so that practical opportunities for personal or electronic feedback would arise. Whilst this instant response did not extend
to an express undertaking towards a risk assessment, it suggested that practical steps would be taken to investigate the issues raised by workforce respondents.

On a similar environmental issue, workforce concerns were expressed about perceptions of lack of mobility in cases in which specific areas were considered beyond the bounds of particular personnel. This led in some cases, to frustration arising from perceived inefficiency where personnel operating at one level of security would be obliged to pass roles on to those with higher level security, leading to perceived issues of job demarcation. Whilst respondents reported recognition that access levels existed for specific and defensible reasons, there appeared to be a perception of inconsistency in approach to security relating to some job roles. This led to a suggested “Best Practice” involving multiple strategies, from the implementation of risk assessment and management to a review of current security policies. Emphasis was placed on management offering assurances of human resource security for employees joining the organisation and/or moving within it. It was also suggested that management introduce and apply express physical and environmental security strategies for access control, incorporating access rights in physical to technical applications. This led to the ultimate suggestion that management undertake a strategic review of the manner in which information systems policies are implemented, to ensure the practical application of social standards, recognising domestic legislation and regulations.

In reply to what would appear to be detailed, multiple suggestions for “Best Practice”, the respondent rejected the need to make any changes in this area of personnel management. In doing so, she pointed to the security critical nature of her department, whereby data integrity was the primary role of both management and workforce. This necessitated the assessment of appropriate levels of access control (largely aligned with job roles) in which there was no room for practical manoeuvre.

This respondent highlighted the need for security vetting to be stringent from the inception of employment and consistently applied throughout the employment lifespan. She further expressed satisfaction that the management approach to levels of security was transparent (citing the workforce perception in response) but she also expressed a view that the strategy was consistent throughout the workforce, rejecting apparent contrary suggestions from workforce
members. In line with her expressed satisfaction that the access control management strategies were appropriate, she defended the current organisational approach to job demarcation.

The previous workforce response requiring justification for the application of access control technology is linked with the subsequent response that social perceptions of technological expense arise that are sometimes perceived as outweighing the practical benefit from access control technology. Context was applied here in suggesting that criminal elements will find a means of falsifying identification to gain illegal access irrespective of the access control measure employed. And perhaps of equal significance in explaining negative workforce responses, parallels were drawn between perceptions of (in some cases) inevitable function-c creep and social exploitation.

This series of workforce perceptions were responded to with suggested practices for management to assure workforce members of risk assessment strategies implemented within the organisation and to illustrate appropriate methods of risk management. The respondent expressed total agreement with this suggestion, linking her response to the previous workforce concerns raised about practical access control management within the department. She suggested that a risk assessment exercise would be useful in addressing the concerns that had been brought to her attention following this research process. She further expressed gratitude towards the process of objective consultation with the workforce, engaged in through this research exercise she suggested that this had provided an opportunity for her to review the system from points of social and ethical perception, in addition to the compulsory legal standards operational within the organisation. She pledged to consider the drafting of a risk assessment exercise that would be transparent throughout the department, whilst alluding to not having an instant answer to the means of implementation. She expressed a determination however to ensure that the exercise, its implementation and feedback would ensure that her objectives of keeping the workforce fully informed of the access control strategy and responding to future workforce perceptions, would be fully achieved.

Remaining with the theme of practical perceptions, the workforce expressed legal concerns about the current application of the Data Protection legislation. Their primary concerns rested with the perceived absence of sufficient rights to store and retain personal data. They also reported suspicion as to the reliability of the current storage and retention systems being implemented within the organisation. The respondents suggested that the existence and
application of the legislation should be reinforced at the organisation, with appropriate staff training about this and subsequent domestic and / or international legislation applicable to them.

This was recognised to be a real concern for the workforce participants involved in this study. It was necessary therefore, to assure those who raised such concerns that the organisational response would strategic and transparent. The associated suggestion for “Best Practice” called for management to “demonstrate and document” the current application of information systems policies illustrating relevant standards, laws and regulations.

On this point, the respondent referred to her previous pledge to initiate risk assessment and response exercises to allay workforce concerns in this area. She tempered this however, with a suggestion that legal regulations are fully implemented within the organisation, but she conceded that perhaps from the perspective of the workforce, there should be greater reference to legal procedures and their social implications. In doing so, she expressed firm agreement that further information should be provided to workforce members, including practical examples to explain how the procedures apply. She also expressed agreement that training in the application and implementation of data protection and associated legal regulations should be applicable to strategic staff.

The discussion in the empirical study developed from issues of legal concern to those of ethical significance. Here workforce representatives reflected on opportunities for employees’ movements to be tracked with tendencies for discrimination between minority groups within the organisation. Specific reference was made to the organisational practise of retina scanning for access control, leading to a perception that visually impaired or blind members of the workforce may perceive themselves to be subjected to unequal treatment.

Whilst it has been described as an ethical concern, this issue clearly spans elements of social, legal and ethical consideration. This led to a suggested “Best Practice” policy capable of securing practical strategies within the organisation that would, not only, be enforced in practise but clearly communicated to all members of the workforce. The suggestion for “Best Practice” here related to organisations having to undertake regular risk assessment exercises and to publish associated risk management strategies. In what appeared to be an emerging point of consensus, the respondent expressed firm agreement towards this suggestion, whilst expressing concern that there should be any perception of unequal treatment towards workforce members within the organisation.
On the penultimate, wider question of social, legal and ethical perceptions of the technology, the investigation proceeded to questions of workforce perceptions of the practical application of ISO/IEC TR 27414-1-2008 and associated funded projects. It focused on the extent of workforce association with biometric access control solutions (specifically iris scanning) and its subsequent (perceived) long-term health implications. There was no specific concern reported about possible health implications beyond one respondent suggesting that (in his opinion) the organisation would not have been permitted to introduce technology that would adversely affect human well-being. However, the issue of the potential to "single out" members of the workforce who may be compromised by the implementation of this technology was re-emphasised by another workplace respondent, leading to the expression of legal and ethical concerns.

The suggestion for "Best Practice" on this point, rested with a recommendation that the organisation introduce and implement transparent communication policies to assess practical risks arising from the implementation of access control technology. Specific reference was made to that associated with risks of discrimination, where appropriate organisational methods for responding to the risks should be identified.

In line with her previous contention that any suggestion of unequal treatment within the organisation was both a surprise and concern for her, the respondent reported firm agreement towards this suggested practice.

Whilst pointing to the detailed consultation emerging from both interview and induction on the issue of access control, she suggested that the proposed fully-informed strategy of risk assessment and response would clarify access control policies and go some way towards justifying their implementation in areas of data security. It was further suggested that this would provide opportunities for clear explanation of the strategies emerging within individual workplaces involving strategic and (in some cases) isolated application to individual members of the workforce. The important addendum here was expressed by the respondent to be a clear explanation of emerging access control management, in a fair and equal way.

The final consideration for empirical enquiry continued the theme of organisational communication. It focused on workforce perceptions of the primary role of consultation, and the
extent to which assurances are maintained of appropriate data management in the procedures for securing biometric access control. The workforce reported positive strategies having been implemented, with personal rights being supported with informed consent in the acquisition, maintenance and storage of personal data for access control management. Whist this strategy was clearly favoured by the respondents, they reported having little or no knowledge of formal organisational policies to comply with the strategies adopted. This led to a suggested “Best Practice” solution based upon the assurance of a supportive role applied by the organisation towards its workforce. It was suggested that there be practical implementation of strategies ranging from the express inclusion of security policies within the working environment to clear procedures to demonstrate management methods in response.

This should be combined with specific access control management practices linking access rights to both physical and technical applications within the organisation. These strategies should be supported with documented information security policies, implemented by the organisation to ensure compliance with standards, laws and regulations towards the dual security of the organisation and its workforce. On this final point, the respondent indicated that the “Best Practice” strategies arising from the empirical investigation were both practical and helpful in highlighting a potential action plan for developing responses to the social, legal and ethical issues emerging from the interviews. She further suggested that the “Best Practice” indicators would be considered on a point-by-point basis. This would form a systematic strategy in which she would attempt to assess risks in relation to their suggested levels of concern. This, she suggested, would best fulfil her overall aim: to practically respond to the issues discussed within this research process.

This point was measured, however, with a contention that whilst she would develop and seek to implement the strategies she had pledged (subject to economies of scale) her experience of management in general, would suggest that the social, legal and ethical perceptions associated with the sensitive and ever-changing nature of access control, would render further review of acceptable management strategies necessary on a reasonably regular basis.
6.5 Presentation of Suggested “Best Practice Model” emerging from representatives of the Selected Samples (Case Studies A and C)

It was suggested at the beginning of this chapter that: “Best Practice” may apply to the process by which organisations balance elements of unique features with those it has in common with other organisations. But it was also conceded that this phenomenon should not be considered to be static. It should be an evolving process fostering the development of new procedures for access control in workplace environments, leading to “Evolving” as opposed to “Best” Practice.

6.6 The Model

This model has emerged from the link between the established access control management Standard within the United Kingdom and responses arising from the empirical studies involved in Cases A and C. The Standard in question is entitled ISO/IEC 27002 Information Technology-Security techniques – Code of Practice for Information Security Management. During the process of empirical investigation, responses from the first cut recommendations were reviewed, following which, six suggested security controls were extracted from the Standard. The controls in question were subsequently applied to participant responses, to form a series of suggested points for “Best Practice”. The combination of interview questions, participant responses, academic consideration and application of the sample of security controls has been combined in this research process to form a suggested “Best Practice Model”. This Model will form a series of recommendations for “Best Practice” within the empirical samples discussed in this thesis (represented by Case Studies A and C). This Model will have the potential to apply to a range of organisations implementing biometric technology for the management of access control.

The Model for application in the current research process emerged from observation of recurring themes and principles in which participant responses and associated “Best Practice” suggestions merged with the series of security controls extracted from the Code of Practice for Information Security Management (ISO/IEC 27002). Whilst the industrial make-up and general nature of individual case studies differed, there are parallels in the participant responses to biometric technology used for access
control management in both organisations. The suggested Model for "Best Practice" was developed during a process of merging common themes and critical mass in principles. This process developed into a series of suggestions considered to be appropriate for both organisations, in addition to having the potential to apply to biometric access control environments on a wider scale.

6.7 Recommendations for "Best Practice" Responding to Elements of Social, Legal and Ethical Consideration in the Management of Biometric Access Control Systems

In formulating the following recommendations, observation was made of recurring themes arising in common between the case studies.

1. **Demonstrate and document the current application of information systems policies.** Ensure that there is a link with individual contracts of employment, both contracts of service and those for services (catering for the typical and a-typical workforce). Demonstration can take place at interview but this must be supported with documented evidence of contractual obligations and detailed security policies in which the workforce will have both statutory and common law obligations to fulfil. The terms of these policies and contractual documents must be clear and fully communicated to the workforce prior to commencement of employment. Any subsequent evidence of failure to comply with formal organisational documents that have been cleared by union representation may be taken to constitute a breach of contract by the workforce, leading to potential dismissal.

2. **Introduce current and developing security strategies to outline management practices.** These strategies should form the basis of consultation with union and staff representation in order for there to be top-down appreciation of both established and developing access control strategies. The policies should be available in documented form upon
workforce request. It is appreciated however, that the types of security strategy implemented by the organisation may be unique to the type of physical and environmental security implemented within that workplace. Again, links should be maintained with relevant contracts of employment and associated legislation, making provision for the protection of human rights and personal freedoms. There should be clear recognition from the outset by both management and workforce of the application of Human Rights, Data Protection, Freedom of Information and Regulation of Investigatory Powers legislation (as applicable to the individual organisational status). Within the sampling frame chosen for current investigation, recognition would span public and private sectors, educational environments, public communications and the aviation industry.

3. Provide specific information to the workforce upon entering, moving within and leaving their place of employment. This procedure retains the “demonstrate and document” theme associated with the management of access control but, in this case, specific social, legal and ethical practices will apply within individual workplaces. Security clearance may be necessary within particular industries at the point of commencing employment. They may relate to Criminal Records Bureaux (CRB) and Home Office (HO) regulations (depending on the status of the workforce member and the nature of employment). From the perspective of movement within employment, there may be social, legal and ethical questions relating to the recognition of and response to job demarcation. Within the process of leaving employment, there may be security issues, necessitating the relinquishing of identification and security clearance documentation, together with any codes or passwords for security sensitive areas. These matters may call for the provision of clearance documentation for formal signature, subject to legal challenge in the future, irrespective of the workforce member’s status at the organisation or his/ her future association with it. Good practice would necessitate the provision of documented consent and release forms to ensure compliance with security regulations at
the organisation and, despite the principle that ignorance of the law does not constitute a defence, the more formal the organisational procedure (in terms of consultation and notification coupled with documentary evidence) the greater the capacity for effective security.

4. **Undertake regular risk assessment exercises and publish risk responses.**
This recommendation arose from a wide spectrum of social concerns relating to access control management. There is a need to conduct regular and consistent risk assessments in parallel with conventions relating to health and safety provision at work. Suspicion has arisen from social scepticism that management intend to introduce a “*total biometric package*” without identifying the nature and implications of this security strategy upon the workforce. The introduction of biometric security systems (from fingerprint to facial recognition and iris scanning techniques) in an environment in which the traditional access control mechanisms had been no more technical than lock and key, pose similar concerns. In addition, the introduction of security scanning (particularly iris recognition) has led to an environment of fear relating to the possible health implications and future effects upon the quality of sight. Evidence has also emerged of tripartite social, legal and ethical concerns associated with the fear of “*function creep*”, in which a security system is introduced within one area of industry, using fingerprint scanning technology but quickly develops throughout the industry, using multiple biometric metrics, in the absence of consultation.

5. **Undertake transparent communication policies.** This recommendation continues the theme of enhancing workforce perceptions of confidence in newly established access control environments. In the case of biometric technology being implemented within the industry, specific workforce fears may arise in particular sectors of employment. This may arise, for example, with experience of false positive or false negative at the registration phase, adversely affecting individual perceptions of the reliability and efficiency of
access control technology. Similarly, the access control method (whether single or multi-modal, single or multi-factor) will potentially affect the long-term perception of the workforce towards secure access control. This may arise for instance where iris or retina scanning technology is applied within the organisation as opposed to the application of less (perceived) compromise (in terms of health implications) arising from fingerprint scanning or facial recognition.

Research has uncovered perceptions of unequal treatment where for example, a potential employee may choose to withdraw from access clearance for conscientious objection to potentially harmful exposure to access control technology. Additionally, an individual with unusual facial features or serious scarring may choose to abstain from access to specific areas and associated opportunities to employment, subject to personal perceptions of segregation or possible discriminatory treatment.

6. **The final recommendation should perhaps appear first in order of significance, that relating to the need for organisations to ensure that management roles are supportive towards the workforce, combined with transparent, tangible evidence of organisational compliance with access control laws, standards and regulations relating to human rights and personal freedoms.** This recommendation combines those cited above and makes specific reference to the need for organisations to respect their management roles towards protecting and enhancing the social, legal and ethical well-being of the workforce. In this respect, human resource management has a clear part to play in the effective and appropriate management of biometric access control rights within the workforce. These management strategies span protection for workplace treatment and respect for human rights, protection of individual privacy and the right not to be discriminated against, enshrined in multiple legislative provisions. These individual rights arise from the Human Rights Act, through Data Protection and the Equal Treatment legislation, all of which exists to bolster the social and ethical protection of the workforce in addition to their legal rights.
established within common law. These rights form the cornerstone of respect for the individual both at work and at leisure. They ensure that the development of subsequent technology within the workplace should not preclude the worker’s liberty to have his or her rights “demonstrated and documented” to preserve constitutional rights to established liberty and personal freedom.

6.8 Chapter Summary and Conclusions

This chapter has provided a definition and assessment of the general concept of “Best Practice” in compiling a series of recommendations towards a model for implementing biometric access control within the case studies under investigation. This began with a series of first cut suggestions being sent to a sample of respondents from (Case Studies A and C) for consideration, comment and assimilation of suggested “Best Practice.” The suggestions were based on a policy introduced by the Department for Trade and Industry (DTI) and published by the British Standards Institute (BSI) in 1995, for the maintenance of “Best Practice” for information security management. This policy was subsequently entitled: ISO/IEC (International Electro-technical Commission) 17799: (27002) Information Technology – Code of Practice for Information Security Management in 2000. Six controls were extracted from this policy and applied to responses gained from the empirical studies conducted in Case Studies A and C. This culminated in the development of six Recommendations for Best Practice. They were made in response to feedback from case study participants towards the social, legal and ethical concerns raised in interviews.
Chapter Seven

Conclusions and Recommendations for Further Research
7.1 Introduction

This thesis has investigated the social, legal and ethical management of biometric technology for access control in workplace environments. It has focused on fingerprint scanning and facial recognition systems in a sample of United Kingdom-based organisations. The organisations have represented a wide-range of employment practices from the educational environment to public communications, a local government department and a representative of the aviation industry.

Before engaging in primary investigation, secondary research was conducted, to gauge the objective perceptions of key players in the field of biometric applications for access control. This was represented by practitioners and members of the United Kingdom Border Agency. This concluded that the application of fingerprint scanning with facial (iris and retina) recognition for access control management should be examined before diverse assumptions could be made about the effects more recent (bleeding edge) technologies. This led the investigation to focus on fingerprint scanning and facial recognition systems primarily, reflecting on a discrete sample of United Kingdom-based organisations. The conceptual framework considered for scoping this research, involved a combination of the Utilitarian principle enunciated by John Stuart Mill, Maslow’s Hierarchy of Needs and the concept of the Psychological Contract.

Before the primary investigation could be undertaken ethical approval was gained through a formal procedure implemented by the Ethics Committee within the School of Management at the University of Wales Institute, Cardiff (cited in: Appendix 1). Following ethical approval, a qualitative paradigm was used in the development and analysis of discourses emerging from interviews with representatives of management and workforce from a sample of United Kingdom-based organisations (represented by Case Studies A, B, C and D). This led to the development of a series of first-cut Recommendations for suggested “Best Practice” in the social, legal and ethical management of biometric access control systems within the selected samples.

The primary investigation was subsequently refined with a smaller sample of respondents (selected from Case Studies A and C), to which the first-cut
recommendations were sent. The responses culminated in the development of a suggested “Best Practice Model” for potential application to all four case study representatives, in addition (potentially) to the wider industrial population within the United Kingdom.

The model was based on elements of a pre-determined Code of Practice (ISO/IEC (International Electro-technical Commission) 17799: Information Technology – Code of Practice for Information Security Management) (Saint-Germain, 2005). A series of six suggested information security controls were extracted from the twelve controls incorporated in ISO/IEC 27002. This strategy was undertaken following analysis of the findings from Case Studies A and C. This led to the development of a series of recommendations for “Best Practice” in ensuring social, legal and ethical approaches towards fostering acceptance of biometric technology within the workplace, in response to the research question:

_How should organisations using biometric access control systems, implement procedures to address social, legal and ethical concerns in the workplace management of specific environments in the United Kingdom?_

### 7.2 Major Findings: Answers to Research Question

The findings from the empirical investigation have been presented separately for this part of the thesis. The themes and their points of overlap have been identified for the development of recommendations for “Best Practice” having been considered in Chapter Six.
Case Study A

The primary findings in response to the investigation undertaken with Case Study A (educational establishment) focused on the biometric system used for access control being non-compulsory in nature. The institution had arrived at the chosen system following in-depth analysis of those available. This had led to the conclusion that the confirmed system represented the most effective on the market at the time. The principal aim was for the institution to fulfil its tripartite obligations to the students, the college and the requirements of the Border Agency. The chosen system used single mode and single factor, in assessment of the potential for system failure, in which case, hard copy registration procedures could be used as a back-up facility.

During the planning and procurement stages for its implementation, there had been consistent consultation between institutional management and suppliers, relating to possible vulnerabilities of the system but in association with staff and student perceptions. Management reported no verbal communication about the nature of the technology and the contingency for system failure. This was perhaps surprising in view of there being no constructive, formal institutional policy in place, other than the practical justification of "need".

The institution reported the use of fingerprint technology for the monitoring of staff and student attendance, with a recognised improvement in attendance from both cohorts since its inception. Upon individual expression of social, legal and ethical concerns in the use and implications of this technology, management was subsequently forced to introduce more stringent verbal communication to allay fears of system malfunction and associated threats.

Once concerns for privacy and personal protection had been allayed with reference to associated legislation, there was general satisfaction in the operation of the system but the application of technology for purposes of monitoring attendance continued to be resisted, on grounds of personal freedom. Management responses remained static however, stressing the application of government edict, preventing opportunities for practical manoeuvre, with the obligation of this institution (in its recruiting of 100%
overseas students) to comply with Border Agency regulations for access control. From the workforce perspective, there was recognition that access security management regulations had been incorporated into contracts of employment, again leaving little or no room for flexibility beyond that potentially associated with union representation and challenge.

Whilst participants acknowledged the need for security strategies of this kind, there was evidence of dissatisfaction that opportunities had not been presented for the workforce to challenge their implementation. This led to elements of disagreement between the workforces with some respondents expressing appreciation that access control systems of this kind are necessary in the effective management of security. In contrast, other respondents had expressed apathy that such systems represented no more practical benefit to the institution than to record staff and student attendance.

**Case Study B**

The major findings from Case Study B (Local Government institution) focused on the increasing link between security and terrorism, leading to the need for management to consider and implement flexible approaches towards access control technology at the workplace. The emphasis on flexibility rested with the need for the workforce to be encouraged to accept access control systems as opposed to perceiving them as being autocratic in nature.

The management response to the use of biometric technology for access control identified the need to develop systems of this nature whilst suggesting that recent economies of scale have prevented a large-scale roll-out of the technology. This had resulted in the current use of swipe card and digital lock systems within some leasing locations of the organisation.

The current application of biometric technology for use in access control environments were reported to be proximity card using fingerprint scanning technology linked to close circuit television. There was emphasis on the need for clear communication in
implementing this technology, with assurances having been undertaken between management and union against the propensity for "function creep".

The major social concerns reported were linked with the perception that personal data may be misused but these concerns were allayed with organisational reference to the Data Protection Principles and their implementation. The current emphasis on the use of swipe cards for access control, as opposed to consistent biometric technologies may have tempered general organisational experience and perceptions of this technology. At the time of conducting the investigation, however, there appeared to be little individual reflection on questions of the social, legal or ethical impact arising from the use of this technology, beyond general concerns for personal rights and the protection of personal identification.

**Case Study C**

The primary findings from Case Study C (Communications environment) began with a focus on both physical and logical security provisions incorporating tangible barriers from security walling and fencing to digital camera monitoring in addition to vehicle recognition and biometric (iris scanning) access control technology. Perhaps most notably, Case Study C presented the first indication of certification in compliance with BS7799: Part 2: 2002 together with Independently Audited National Approval Council for Security Systems. The multi-level strategy to access control led to reports that no strategic security policies had been changed in response to the terrorist attack on the World Trade Centre in September 2001, because an optimum level of security has been consistently maintained at this organisation.

The system was reported as representing a single-modal (iris scanning) and multi-factor facility, whereby the use of card access in conjunction with biometric technology, provides a fall-back position in the event of system failure. This is supported with fortnightly risk assessment and review procedures in which security levels at strategic places within the building are assessed and the technology is consistently maintained at a security level in which iris images are capable of being discriminated between from
point of enrolment to point of subsequent match. The investigation revealed that consultation was taking place towards the question of "need" for this level of security at strategic places, whilst there was no report of the current need for consistent access control strategies to be maintained at that level of security.

The overall management perception was reported as representing 100% workforce acceptance of and commitment to the current security technology implemented within this organisation. This led to reports that beyond the application of more recent hardware and software, there were no further plans to enhance the system used beyond stated procedures for technology-refresh.

**Case Study D**

The final organisation investigated (represented by Case Study D: representative of the Aviation industry) was shown to have a more static approach to access control security and its management with its compulsion to apply set standards for the access control environment within the National Aviation Security Policy (NASP), implementing magnetic code access control for discrete zones.

In compliance with government regulations towards the consistent maintenance of access control however, it was suggested that social, legal and ethical acceptance of the technology within this environment is dependent upon a balance being maintained between the perceived need to engage in security management and that to avoid any perception of fostering a "siege state."

On the question of using body scanning equipment, it was reported that the decision had been taken to avoid its implementation based on concerns of potential social intrusion and individual perception of the surveillance state. In making this point the participant expressed his (management) view that images captured for subsequent identification are only as accurate as those stored on driving licences or other traditional areas of image recognition, emphasising his perception that this technology should never be considered to be 100% foolproof.
Whilst this environment reported the use of magnetic strip as the primary source of access control procedure currently, consideration of subsequent biometric technologies focused on the use of fingerprint scanning and facial imaging, in the absence of financial support from government to develop market and implement a more comprehensive variety of biometric modes. On wider reflection towards the use of biometric technology for access control it was considered that, in focusing on acceptable social, legal and ethical implementation of this technology, perhaps it is only as useful as its management.

The ultimate finding linked (again) with the concept of perceived “need”, in which it was reported that in the event of proven need, the technology should be accompanied by an objective, well-informed policy, communicated to all staff. This suggestion was based upon the perception that a transparent management approach would reduce workforce suspicion about the liability of this technology to be applied by management and / or government in an autocratic way.

7.3 Contributions to Theory, Practice and Methodology
The academic approach employed in this series of investigations rested on the primary principles of institutional theory and the technology acceptance model in forming a foundation for the themes adopted in the semi-structured questions used for empirical investigation. The themes employed within the questions and principles for subsequent analysis rested with a combination of the principle of Utilitarianism (in interviews with both management and workforce) Maslow’s Hierarchy of Needs (in interviews with workforce representatives) the concept of the Psychological Contract (in interviews with both management and workforce). The rationale for adopting this tripartite theory rested with the methods by which each of the three principles referred to may be aligned with perceptions from management and workforce respectively.

The underlying theory for the investigation focused on a dual approach, relating to institutional theory and the technology acceptance model, with the latter focusing on the process by which rules, norms and routines have the capacity to become authoritative
guidelines for social behaviour. The importance of this theory to the research in question rested with its consideration of how such rules and norms created, implemented and developed over time, may facilitate the development of stability in social life. This theory (also referred to as adaptive theory) was considered appropriate in addressing questions of organisational approach towards the use of biometric access control technology. More specifically, however, it was considered in assessing methods by which organisations choose to implement and adapt this technology towards the social, legal and ethical acceptance of the workforce.

The Technology Acceptance Model was chosen in this investigation due to its alignment between technology usage behaviour across a broad range of end-user applications and user populations. It was considered that a combination of these theories would set a firm foundation for theoretical assessment to support the empirical response to the research question: *How should organisations using biometric access control systems, implement procedures to address social, legal and ethical concerns in the workplace management of specific environments in the United Kingdom?*

In setting the appropriate forum for the research path, a clear appreciation of these theories was considered necessary before empirical investigation could begin. In preparation, academic observation was made of a pilot study having been conducted in 2004 to determine the social perception of biometric access control in an American stadium hosting athletic events, focusing on system security, performance and acceptance. This had resulted in the development of a Dynamic Acceptance Model for the Re-evaluation of Technologies (DART), subsequently assessed and considered in the framing of semi-structured interview questions for the current investigation.

Having set the theoretical background for the current study, a suitable framework for deciding on the appropriate development and management of interview questions with management and workforce was considered. This involved aligning theoretical principles with case study respondents, resulting in the application of a tripartite study into the social, legal and ethical impact of biometric implementation for workplace access control. From this emerged the theory of Utilitarianism being assessed as
appropriate in the design of semi-structured interviews with management and workforce, whilst Maslow’s Hierarchy of Needs was considered in the design of questions addressed specifically to workforce members and the concept of the Psychological Contract was applied to both management and workforce.

The rationale for the application of this philosophy to management and workforce perceptions rested with the principle of Utilitarianism contending that *the useful is the good*. The philosophy of Utilitarianism is based on the association of the greatest happiness for the greatest number of people. The empirical investigation focused on the development of a management strategy in which the greatest satisfaction of the greatest number of workforce members would be sought, whilst recognising that (inevitably) there would be some members of the workforce who would resist the application of this technology within access control environments. In considering this philosophy from the viewpoints of both sets of participants, it was decided that a balance would have to be drawn between an objective assessment of management strategies and workforce responses.

The second theoretical consideration in the framework rested with Maslow’s Hierarchy of Needs, focusing on the need to foster human motivation. The rationale for concentrating on workforce perceptions at this point rested with the recognition that, whilst management have to find ways of motivating the workforce towards accepting the implementation of this technology, there are specific workforce needs that are not communicated to management. In response to this, it was considered that the most effective method of assimilating social, legal and ethical perspectives from the workforce would be to focus on encouraging workplace participants to freely discuss their specific needs, fears and perceptions.

Whilst taking care to avoid leading the workforce into any specific suggestion of “Need” the research process encouraged interviewees to explain the issues raised. They were most notably associated with safety and security and the need to be protected from threats of physical and emotional harm, potentially arising from the application of new technology in the access control process.
The third and final application of theory to the practical investigation related to the association of the Psychological Contract with the perceptions of management and workforce, towards the implementation and practical management of access control technology within the workplace. This philosophy focused on the mutual expectations of individuals within any relationship. Most notably in the context of this investigation, this considered the aspects of changing expectations with time and technological development were considered. This was a primary consideration in the investigation conducted with both management and workforce, leading to questions about the methods by which contractual obligations should be adhered to and methods by which acceptance or rejection of obligations would impact upon the working relationship. The psychological contract was considered to play a primary role in establishing management recognition of social, legal and ethical obligations towards the workforce and reciprocal workforce obligations to objectively respond to social, legal and ethical management requirements towards the development of this technology within the workplace.

Having outlined the contributions made by this research process towards theoretical principles, this section will conclude with an indication of the associated contributions towards academic practice. The practical elements arising from the study have been associated with the development of a suggested “Best Practice Model” for the application of management and workforce towards the development and implementation of biometric access control systems within the workplace. This has been based upon the selection of six (from twelve) suggested information security controls contained in ISO/IEC 27002 Information Technology – Security techniques – Code of Practice for Information Security Management.

1. Risk Assessment and relevant management;
2. Security Policy and management;
3. Human Resources Security – for employees joining, moving and leaving the organisation;
4. Physical and environmental security – protection of facilities;
5. Access Control – management of access rights to physical and technical applications; and

The controls were selected following empirical responses from management and workforce representatives within the two case studies (Case Studies A and C) selected for the application of first cut recommendations. The selected controls were aligned with the theoretical background (relating to Institutional Theory and Technology Acceptance) previously discussed, and subsequent tripartite principles (represented by Utilitarianism, Needs and the Psychological Contract).

This conceptual framework was practically applied towards the compilation and development of a series of recommendations towards a suggested “Best Practice Model” aligned with the selection of (six) suggested information security controls. They combined the theoretical background and framework principles with the practical application of ISO/IEC 27002 Information Technology – Security techniques – Code of Practice for Information Security Management.

7.4 Limitations of this study

The security sensitive nature of this investigation has, to some extent, made limitations inevitable but this had been appreciated as having the potential to create risk from the outset. The aim and objectives were therefore framed to facilitate a balance between ensuring that the outcomes are representative of the selected sample and manageable for the research process, in order that objective recommendations may be made for the compilation of an (objective) “Best Practice Model.”

In embarking on this research path it was appreciated that any investigation into biometric access control management is liable to present social and ethical dilemmas for management. This issue was pursued from the outset, with a number of experts in the field of practical access control management, including the pilot exercise. In attempting
to ensure an appropriate balance between addressing sensitive management-related questions and taking an objective view about how they were likely to be received in practice, the responses gained were reflected upon from those received following the pilot investigation. The pilot questions were refined before conducting semi-structured interviews with the four case study participants chosen for empirical investigation. The need to maintain an objective approach and to remain non-judgemental in the manner of asking questions and receiving participant responses was appreciated throughout the process of empirical investigation.

Whilst the limitation referred to above, was one of the primary sources of concern, this was not initially experienced with either management or workforce participants in the four case study samples selected for investigation. But, upon the subsequent refinement of a sample of two from the original four case study participants to whom a series of first-cut suggestions towards achieving social, legal and ethical acceptance of access control management strategies was sent, there was some evidence of "defensive" response. This defence mechanism was particularly (but not wholly) evident in management responses, where it would be suggested that a variety of practices had already been implemented, whilst reciprocal workforce respondents had suggested to the contrary.

This experience led to an element of compromise having to be considered in compiling an objective set of recommendations for a suggested "Best Practice Model" in the selected sample. In response to this, an objective strategy was decided upon in an attempt to minimise the possible limitations within management and workforce responses. This involved a process of reflection on the responses of both sets of respondent (applying the theoretical framework previously discussed). The principle of Utilitarianism was reflected on in reviewing management and workforce responses, with Maslow's Hierarchy of Needs being applied solely to the workforce perception and the theory of the Psychological Contract reflected upon and subsequently applied to the (perceived) relationship between management and workforce on the question of the social, legal and ethical management of biometric access control systems.
This emphasis on balancing empirical responses with established, theoretical philosophies has, in the questions posed by the semi-structured interviews, gone some way to ensuring that the inevitable social limitations associated with gaining an objective set of responses in this kind of security sensitive research area, has been kept to a minimum.

The other limitation encountered in this study related to an area for which pre-planning had not been possible and there was no practical (instant) opportunity for contingency. This arose following empirical investigation with a management respondent from one of the (initial) four case study respondents. This respondent had participated in the initial interview process in an enthusiastic and knowledgeable way but unfortunately, he subsequently suffered long-term ill-health, resulting in a successor having to be contacted. With the workload she had recently undertaken, she expressed less informative engagement in this research area. This led to one of the reasons for the rationale adopted in choosing to refine (the original) four case studies to two, in order to compile and send a series of first-cut recommendations for suggested "Best Practice" and objective response. It was considered that having worked closely with the subsequently selected case study participants (at both management and workforce levels), the associated responses would be a more reliable and representative forum from which to compile a series of recommendations towards a "Best Practice Model" for the social, legal and ethical management of biometric access control systems. In the case of the other (initial) respondent chosen to be eliminated from the final recommendations for "Best Practice", again, this decision arose from a perception towards limitation in the practical (objective) participation of management.

This emerged from the initial semi-structured interview, during which, whilst again the management response was highly informative and interesting, there was a suggestion that his security sensitive role, specifically in areas that (at the time of the interview) represented a real security threat within the locality and to himself. He therefore suggested that if he were to be identified as being connected with research into security management and control he could place himself at personal risk. This led to the case study in which he had been involved being eliminated from the provision of refined
recommendations. This perceived reticence was considered as having the potential to limit the practical responses and hence the ultimate validity of data presentation and subsequent analysis from this case study environment. The position was defended irrespective of documented assurances from the University towards the protection of anonymity for every research participant, because this participant perceived inherent management fear of subsequent publication of research data.

Beyond the practical limitations considered above, few other limitations were encountered beyond the inevitable time constraints arising from engaging in research at this level whilst pursuing a full-time lecturing role. And, as has been discussed, an element of practical limitation inherent in the chosen research topic and subsequent process had been predicted. In response to this, the research path has been managed so as to ensure that limitations were kept to a minimum and (upon reflection) this appears to have been achieved in the relatively minimal limitations arising from what is a potentially security sensitive area of research.

7.5 Opportunities for Further Research

Opportunities for further research arose in this study from a relatively early stage in the investigation. It soon became evident that the prospect would emerge of using this initial series of case studies as a foundation for the overall research process, whilst providing subsequent opportunities to apply a similar philosophy to a separate sampling frame. The designing of a consistent conceptual framework from which to select a relevant sample for this investigation (using theoretical concepts of Utilitarianism, Needs and the Psychological Contract) ensured that an alternative sample could be selected for the subsequent application of semi-structured interviews with representatives of management and workforce. This could result in pursuing subsequent perceptions from each body of respondents on questions of the social, legal and ethical management of biometric access control systems.

Following the pilot study, this investigation had concentrated on what had been considered to be a “representative sample” of environments using biometric access procedures, from the civil aviation authority, a public communications organisation, a
local government department and an educational establishment, from a relatively wide variety of industry.

This study has formed a backdrop for investigation into fingerprint (iris and retina) scanning and facial recognition systems within established environments, with opportunities presented for future (similar) investigations to be undertaken with alternative samples, applying the more advanced "bleeding edge" access control technologies. This would provide opportunities for research to continue in these areas, using the same theoretical principles and conceptual framework for the future analysis of social, legal and ethical perceptions of both management and workforce in more disparate areas of industry and commerce.

In recognition of the possible dissemination of research into commercial areas, opportunities would be presented to add a further layer (or sector) to the investigation by including (for example) consumers, in the empirical process. This could include new facets of perception in considering the future development of biometric access control facilities and their "acceptable" implementation into workplaces. Whilst this would necessitate a change of emphasis in the aim and associated objectives of the current investigation, it would be beneficial in developing a general body of knowledge and reflection on responsible considerations for ensuring that access control procedures are socially appreciated in securing the privacy and human rights of personnel. This would perhaps serve the tripartite purpose of ensuring appropriate management, whilst assisting in workforce acceptance and enhancing the perception of society in general towards the value of biometric access control facilities. This would apply both in their present form and towards their future development into new biometric applications for the security of people and organisations in the future.

In implementing biometric access control systems, there is also potential for consistent reflection on elements of "Best Practice." This could apply both within the suggested Model and in subsequent reflections on and developments in management strategy towards social perceptions, legal regulations and ethical standards as this area of security provision, with the future development of more refined technology.
In the final analysis of opportunities for further research, it is considered that this area of investigation, whilst being subject to suggested recommendations for “Best Practice” in the current study, is constantly changing. The theory of “Best Practice” should be (more correctly) referred to as “Evolving Practice” with the future development of new processes to secure access control in workplace environments.
REFERENCES

AND

BIBLIOGRAPHY
References

Alderfer (envisonsoftware.com/articles/ERG_Theory.html) (Accessed 21/10/09)
BITE: www.biteproject.org (Accessed 25/01/10)
Clarke, R. (2001) Biometrics and Privacy, Visiting Fellow, Department of Computer Science, Australia National University, Notes of 15th April 2001
de Hert, P. (2005) Biometrics; Legal issues and implications: Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission
Emilio.mordini@cssc.eu

European Standards and Workshop Agreements (ISO/IEC Guide 71, Guidelines for Standards)

Firm’s biometric records can be hacked; Computer and Internet Security News (19th March 2008) http://www.techworld.com (Accessed 12/05/08)


HIDE (www.hideproject.org) (Accessed 25/01/10)


ICO, The use of biometrics in schools, V1.1 August 2008


JIS X8341, 2004

IFSEC Conference (Information Security) Birmingham NEC, 24th March, 2009

IFSEC Global Information Systems Conference, Birmingham Exhibition Centre, March 2009


ISO/IEC TR 24714-1: 2008 Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies


International Biometric Group, www.biometricgroup.com (Accessed 03/04/09)

International Conference on Automatic Face and Gesture Recognition (FG'06)
University of Southampton, UK, April 10-12th, ISBN 0-7695-2503-2
Networked Society, Kluwer Academic Publishers
IEEE Transactions, January, vol. 14, issue, 1: 4-20
Engineering 586, University of Virginia, Charlottesville, VA.
https://toolkit.itc.virginia.edu/cgi-local/tk/UVA_SEAS_2005_Fall_ECE586
Kablenet (2007) www.theregister.co.uk/2007/02/20/biometric_travel_plans_criticised
(Accessed 25/07/08)
Lancaster, H. (2009) As biometrics move into the public sector, learn how they can be
applied, http://submityourarticle.com (Accessed 01/10/09)
Marks (2007)
Liability Insurance Costs? HR and Recruitment (Ireland)
www.hri.ie/hr/index.php?option=com_content&view=article (Accessed 29/7/09)
White House Staffer, http://www.nationaldefensemagazine.org (Accessed 9th June,
2010)
pp. 38-39
Mazumdar, Subhra; Dhulipala, Venkata (2008) Biometric security using fingerprint
recognition. (PDF) University of California.San Diego:
McIntosh (2008) “High security
biometric access control in a leading financial institution”, paper presented at the
Biometric Conference, Westminister London, 22nd October
Minutia vs Pattern Based Fingerprint Templates
n/Whitepapers/pdf/9/M_vs_P-(Accessed 21/11/10)
www.information-age.com (Accessed 26th April, 2008)
March/April, www.baselinemag.com (Accessed 28/6/10)
11th, 2008: 25
29/7/09)
Essays on Bentham and Selections of writings from Jeremy Bentham and John Austin,

232


Myers, M. (2009) Qualitative Research in Business and Management, Sage


Naysmith, S. 2009. ‘Don’t sleepwalk into Big Brother surveillance, schools warned’, The Herald, 13 January, at www.theherald.co.uk/features/otherfeatures/display.var.2481176.0.Dont_sleepwalk_into_Big_Brother_surveillance_schools_warned.php (Accessed 12/02/10)


Office of the Commissioner for Human Rights; General Assembly Resolution 2200A (XXI) 16th December 1966, entry into force 23rd March, 1976 in accordance with Article 49 Geneva: OHCHR


Preston, F. (2005) Police hope Biometrics will provide arresting results; ZDNet UK, (http://news.zdnet.co.uk) (Accessed 01/10/09)

Preston, Dr. F. Senior Professional at Sagem Securite, Basingstoke, UK (2009) email (17th February 2009)


Ritzer ed. Thousand Oaks, CA, Sage, 408-414
Roberts, J. (2009) EU as Big Brother is a threat to liberty, Daily Mail (London), June 22nd, 2009: 26
Shontz, Douglas (2010) DNA as part of Identity Management for Department of Defense, occasional paper, RAND National Defense Research Institute, Santa Monica, CA
Smart, J.C.C. and Williams, B. (1973) Utilitarianism: For and Against, Cambridge University Press
Stephenson, P. (2007) Group test: Biometric tools: From fingerprint scanning to facial recognition, these solutions provide high security access control to networks, PCs and buildings. Will passwords soon be a thing of the past? S.C. Magazine: 64

Williams, B. (1973) A Critique of Utilitarianism, Routledge
Wolcott, H.F. (2001) Writing up Qualitative Research, Sage

Bibliography

Macmillan
Myers, M. (2009) Qualitative Research in Business and Management, Sage
Yin, R. (1994) Case Study Research (Design and Methods) Sage

Electronic Resources

http://www.identitytech.com/Technology/Facial-Recognition/About/Facial (Accessed 10/06/10)
http://www.boozallan.com (Accessed 10/06/10)
http://ccert.edu (Accessed 10/06/10)
http://cilab.upf.edu (Accessed 10/06/10)
www.nacccq.ac.nz (Accessed 6/7/10)
http://webspace.ship.edu/cgboer/maslow.htm (Accessed 17/09/09)
www.cipd.co.uk/subjects/empriMns/psychntpsychcontr.htm (Accessed 29/07/09)
www.riseproject.eu
http://www.vome.org.uk (Accessed 04/02/10)
www.observer.guardian.co.uk (Accessed 03/04/09)
www.the-register.co.uk (Accessed 01/01/09)
www.file???\E:\Interpretivism.htm (Accessed 7/11/08)
si.umich.edu
chass.ncsu.edu
mujersana.ca.msproject/framework/-e.php
utilitarianism.com/mill1.htm
netmba.com/mgmt/ob/motivation.maslow
ship.edu/cgboer/maslow.htm
envisionsoftware.com/articles/ERG_Theory.html
cipd.co.uk/subjects/emprelns/psycentrct/psycontr.htm
personeltoday.com/articles/2006/11/21/38212/trade-secrets-protecting-the-
psychological-contract.htm
(file:/U:/PhD Chapter 2 - Approach / Recruitment and Staffing – Trade secrets
Protecting) (Accessed: 30/01/2009)
useit.com/alertbox/20030825.html (Accessed: 11/02/09)
www.bu.edu/wcp/Papers/Mind/MindMech.htm (Accessed: 12/02/08)
(file:/U:/PhD Chapter 2 - Approach\Hierarchy of Needs.htm)
(http://www.lep.utm.edu/m/millsjs.htm) (Accessed: 09/02/2009)
APPENDICES
Appendix 1: Application for Ethics Approval

All Principal Investigators (PI) undertaking a research project which involves human participants should complete and sign this application form.

The document Guidelines for obtaining ethics approval gives full details of how to complete this form and is available via the research pages of the UWIC website. You should refer to this document in order to avoid unnecessary delays with your application.

As a PI, you are responsible for exercising appropriate professional judgement in this review and for operating within UEC (and any School and professional) guidelines in the conduct of the study.

Participant recruitment or data collection must not commence until ethics clearance has been obtained.

<table>
<thead>
<tr>
<th>Principal Investigator:</th>
<th>This should be the name of the student</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor (if student project):</td>
<td>This should be the name of the supervisor</td>
</tr>
<tr>
<td>School:</td>
<td>Cardiff School of Management</td>
</tr>
<tr>
<td>Type of researcher:</td>
<td>Undergraduate Student/Masters student</td>
</tr>
<tr>
<td>Student Number (If applicable):</td>
<td>Insert student number</td>
</tr>
<tr>
<td>Programme enrolled on:</td>
<td>Insert degree title</td>
</tr>
<tr>
<td>Project Title:</td>
<td>Use a working title – it can changed later if necessary</td>
</tr>
</tbody>
</table>
PART ONE – ETHICS REVIEW CHECKLIST

<table>
<thead>
<tr>
<th>ERC1:</th>
<th>Will the study involve NHS patients or staff?</th>
<th>No</th>
</tr>
</thead>
</table>

If YES, you do not need to complete Part Two of this form. Instead, an application for ethics approval must be submitted to the appropriate external NHS Research Ethics Committee. Complete Declaration A overleaf and forward a copy of your NHS application plus Part One of this form to your School Ethics Committee for information.

<table>
<thead>
<tr>
<th>ERC2:</th>
<th>Does your research fall entirely within one of the following three categories:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Paper-based, involving only documents in the public domain</td>
</tr>
<tr>
<td></td>
<td>- Laboratory based, not involving human participants or human tissue samples (eg electronics, chemical analysis)</td>
</tr>
<tr>
<td></td>
<td>- Practice-based, not involving human participants (eg exhibitions, curatorial, reflective analysis, practice audit)</td>
</tr>
<tr>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

If YES, you do not need to complete Part Two of this form. Instead, complete Declaration B overleaf and send the completed form to your School Ethics Committee for information.

If NO, you must complete Part Two of this form and submit your application (Part One and Part Two) to your School Ethics Committee for consideration.
**DECLARATION A**
I confirm that the information contained in this form is correct

My research involves human participants and ERC1 indicates I must obtain ethics clearance from the appropriate external health authority ethics committee.

Signature of Principal Investigator:

| Date: | Click here to enter a date. |

**DECLARATION B**
I confirm that the information contained in this form is correct

My research falls entirely within the categories described in ERC2 and I do not need to take further action to obtain ethics clearance.

Signature of Principal Investigator:

| Date: | Click here to enter a date. |

**Brief synopsis of project:**
This box only needs to be completed if you are not doing primary data collection with people, e.g. using questionnaires, interviews or focus groups.

**FOR STUDENT PROJECTS ONLY**
I confirm that I have read and agreed the information contained in this form

| Name of Supervisor: Name of supervisor | Date: Click here to enter a date. |

Signature of Supervisor:

**School Research Ethics Committee use only**

<table>
<thead>
<tr>
<th>Considered and supported</th>
<th>Considered and not supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Click here to enter text.</td>
<td>Date: Click here to enter a date.</td>
</tr>
</tbody>
</table>
PART TWO – APPLICATION FOR ETHICS APPROVAL

<table>
<thead>
<tr>
<th>Expected Start Date:</th>
<th>18/11/2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approximate Duration:</td>
<td>12 weeks</td>
</tr>
<tr>
<td>Funding Body (if applicable):</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Other researcher(s) working on the project</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Does your project require ethical approval from an NREC or other body?</td>
<td>No</td>
</tr>
<tr>
<td>If yes, please name the NREC or other body</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Does your project use Human Tissue?</td>
<td>No</td>
</tr>
<tr>
<td>Has CRB clearance been given?</td>
<td>No</td>
</tr>
<tr>
<td>If yes, which organisation holds details of the check?</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

DECLARATION

I confirm that the information contained in this form is correct
Signature of Principal Investigator: Date: 28/10/2010

FOR STUDENT PROJECTS ONLY

I confirm that I have read and agreed the information contained in this form
Name of Supervisor: Name of supervisor Date: 28/10/2010
Signature of Supervisor:

Research Ethics Committee use only

Decision reached:
- Project approved
- Project approved in principle
- Decision deferred
- Project not approved

1 In cases where a CRB check has been sought by an external organisation, confirmation from that organisation that a satisfactory check has been received is required by UWIC at application stage.
A - PROJECT DETAILS

A1 In order to give members of the ethics committee some idea of the nature of your research, please answer the following questions with regard to this project:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will you take blood or tissue samples from participants?</td>
<td>No</td>
</tr>
<tr>
<td>Will the study involve prolonged or repetitive testing OTHER THAN repetitive training exercises of a type which form part of the participants normal activities (such as athletics or music training)?</td>
<td>No</td>
</tr>
<tr>
<td>Are drugs, placebos or other substances (eg vitamins) to be administered to participants?</td>
<td>No</td>
</tr>
<tr>
<td>Could the study induce physiological or psychological stress or anxiety significantly greater than the participants are likely to experience in their daily lives?</td>
<td>No</td>
</tr>
<tr>
<td>Does the study involve participants who are unable to give informed consent?</td>
<td>No</td>
</tr>
<tr>
<td>Will the study involve children? (NB: Projects in professional practice involving those under the age of 18 in a public place (in school or a statutory setting) with the relevant permission are exempt)</td>
<td>No</td>
</tr>
<tr>
<td>Is pain or more than mild discomfort likely to result from the study?</td>
<td>No</td>
</tr>
<tr>
<td>Will financial inducements, other than reasonable expenses and compensation for time, be offered to participants?</td>
<td>No</td>
</tr>
<tr>
<td>Will deception of participants to necessary during the study?</td>
<td>No</td>
</tr>
</tbody>
</table>
A2 Briefly describe the rationale behind your project
We want to know the academic justification and background for your study and what are the benefits of doing this research, e.g.: enhanced understanding of motivation for X.

A3 What are the aims of the research?
In this section you should explain your main research question and the specific objectives of your study.

A4 Will you be using an approved protocol in your project? No
A5 If yes, please state the name and code of the approved protocol to be used
Not applicable.

If your project does involve the use of an approved protocol, please indicate when answering the following questions, which areas of your study are covered by the protocol
Not applicable

A6 What methods of data collection and analysis will you adopt?
Describe and justify the overall design of the project and the methods of data collection and analysis which will be used. Provide a brief summary of the nature of the participants’ involvement, e.g. participants will be interviewed about their motivations in relation to X OR participants will be asked to complete a questionnaire. The committee needs to know:

Why this is necessary
Where it will take place
How long it will take
How many sessions need to be attended
How long the interval between sessions will take place

A7 What remuneration (if any) will be offered to participants?
Full details of any remuneration are required. Payment of reasonable expenses covering travel and subsistence is fine. Recompense for time committed is also fine. Where large incentives are offered the committee will have to assure itself that participants are not being encouraged to take risks that they would not otherwise take.

A8 From which group(s) will participants be recruited and what sampling method and criteria will be used?
There should be an inclusive approach to recruitment. Detail any limits to recruitment and justify limits. You should indicate whether the gender mix, ethnicity, disability or other socio-economic factors will affect the recruitment strategy to the study. Sampling methods and inclusion/exclusion criteria and how they will be applied (e.g. screening or self-exclusion) are important

A9 How many participants will be involved?
Please state how many participants you intend to recruit.

A10 Where and how will the participants be recruited and what method of initial

---

2 An Approved Protocol is one which has been approved by UWIC to be used under supervision of designated members of staff; a list of approved protocols can be found on the UWIC website [here](#).
<table>
<thead>
<tr>
<th>C1</th>
<th>Will informed consent be sought from participants?</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2</td>
<td>IF NO, explain why informed consent will not be sought</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the research involved observing people in their day-to-day lives, e.g. in groups in public, then consent may not be an issue.</td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>IF YES, describe how informed consent will be obtained and attach copies of relevant documents</td>
<td></td>
</tr>
<tr>
<td></td>
<td>People must have the right to choose whether or not they will participate in a study. INFORMED CONSENT is therefore central to the ethical conduct of research involving people. Participants must be give an explanation (oral and/or written) about what participation entails in SIMPLE NON-TECHNICAL TERMS, what is involved, the potential risks and hoped for benefits. Reasonable time must be given for the participant to consider this information and to consult others</td>
<td></td>
</tr>
</tbody>
</table>

---

**B – POTENTIAL RISKS**

<table>
<thead>
<tr>
<th>B1</th>
<th>What potential discomfort or inconvenience to the participants do you foresee?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For research involving interviews and questionnaires any risk of psychological or social ill effects should be considered.</td>
</tr>
<tr>
<td>B2</td>
<td>How do you propose to deal with the potential risks?</td>
</tr>
<tr>
<td></td>
<td>How will you deal with the risks you identify in B1?</td>
</tr>
<tr>
<td>B3</td>
<td>Do you intend to use a questionnaire to ascertain an individual’s level of physical fitness or health before accepting them as a participant? If yes, please give details.</td>
</tr>
<tr>
<td></td>
<td>For CSM-type projects the answer to this question is likely to be no.</td>
</tr>
<tr>
<td>B4</td>
<td>What potential risks to the interests of the researchers do you foresee?</td>
</tr>
<tr>
<td></td>
<td>Consider risks to the researcher, e.g. if undertaking face to face interviews in Queen Street on a Saturday night.</td>
</tr>
<tr>
<td>B5</td>
<td>How will you deal with these potential risks?</td>
</tr>
<tr>
<td></td>
<td>Please explain how the risks in B4 will be dealt with.</td>
</tr>
</tbody>
</table>

---

**A11 What previous experience of research involving human participants relevant to this project do you have?**

Obviously students are unlikely to have had any previous experience so no is a perfectly valid answer here but supervisors will provide an outline of their previous experience below.

**A12 Student projects only**

*What previous experience of research involving human participants relevant to this project does your supervisor have?*

A supervisor may have undertaken a similar study for their own research and may have supervised similar projects over a period of time.
if necessary. Except for questionnaire-based studies the participant should be asked to sign a consent form.

<table>
<thead>
<tr>
<th>C4</th>
<th>If you are using an approved protocol, has the approved wording for participants been included in your Participant Information Sheet?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not applicable..</td>
</tr>
</tbody>
</table>

C5 If NO, why not?
Not applicable.

C6 If there are doubts about participants’ abilities to give informed consent, what steps have you taken to ensure that they are willing to participate?
Working with vulnerable adults is something that requires special consideration. Generally this is likely to be Not applicable for CSM-type studies.

C7 If participants are aged under 18, describe how you will seek informed consent
Our research generally does not involve people under the age of 18.

C8 How will consent be recorded?
Consent Forms will be collected from all participants and will include specific boxes of consent relating to the research e.g. audio/video recording, being re-contacted etc. Consent forms will then be copied/duplicated and given to participants along with the information sheet.

D – OTHER DETAILS

D1 Will participants be informed of their right to withdraw without penalty? We would expect the answer to this to be Yes.
If no, please detail the reasons
Hopefully this is not applicable.

D2 How will you ensure participants’ confidentiality and anonymity?
If your data will be shared, e.g. with a sponsor, this must be clearly stated on the information sheet. If you want to re-contact people you should ask participants to consent to this on the consent form. PIs are expected to respect participant confidentiality except if disclosure is required by law, e.g. if there is a threat of abuse to a child or if there is professional misconduct. Reasonable steps should be taken to ensure anonymity of participating individuals and organizations, e.g. by identifying participants by a code which is kept separate to the data. If you cannot ensure anonymity this should be made clear to the participants.

D3 How will issues of data storage be addressed?
How will the data be held and who will have access to it? All information gathered should be retained by the PI and stored in a secure location and accessible for inspection if requested for a period of FIVE YEARS after the work is completed. Participants have the right to inspect the record of their participation.

D4 Are there any further points you wish to make with regard to the proposed research?
If there are any other issues they should be detailed here together with how they will be addressed.
NB: When submitting your application, in addition to this form your School Ethics Committee will expect to see copies of the documentation you will use during your project. Depending on what your project entails, this may include:

- Participant information sheet (See Section C)
- Participant consent form (See Section C)
- Parents information sheet (See Section C)
- Parents consent form (See Section C)
- Participant questionnaire (See A6)
- Health questionnaire (See B3)
- Letter to the organisation at which research will take place

Refer to the document *Guidelines for obtaining ethics approval* for further details on which documents you should provide and exemplar forms for your reference when compiling this information.
Appendix 2: Participant Acknowledgement and Consent Form

PARTCIPANT ACKNOWLEDGEMENT AND CONSENT FORM

Nature of Research: Thesis submitted to the University of Wales Institute, Cardiff in fulfilment of the requirements for the degree of: DOCTOR OF PHILOSOPHY (PhD) (2008-2011)

Research Question: How should organisations using biometric access control systems, implement procedures to address social, legal and ethical concerns in the workplace management of specific environments in the United Kingdom?

Principal Investigator: Lynne Norris-Jones (Department of Information Systems and International Studies, Cardiff School of Management)

Participant Acknowledgement and Consent Form:

1. I WOULD / WOULD NOT be prepared for my name to be included in the formal bound version of this document;

2. I WOULD / WOULD NOT be prepared for the name of my institution to be included in the formal bound version of this document;

(Please delete as appropriate)

Signature of Participant (to remain anonymous):
Appendix 3: Refined Questions Following Piloting of Semi-Structured Interview

BIOMETRIC ACCESS CONTROL FOR WORKPLACE MANAGEMENT

STATEMENT OF PURPOSE

To investigate the development of biometric access control systems (primarily relating to fingerprint scanning and facial recognition) in a sample of United Kingdom organisations.

Please be aware that you may decline to answer any of the questions in this interview and you have the right to remain anonymous.

Conducted with MANAGEMENT

Name of Organisation: 
Date of Interview: 
Name of Interviewee: 
Email address: 

1. Have you used biometric technology for access control in your organisation?

   If you answered yes to Qu. 1: what did you use before biometrics?

   PLEASE GO TO QUESTION 2

   If you answered no to Qu. 1: what types of access control do you use (if any)?

   PLEASE GO TO QUESTION 11
2. Do you use a single (e.g. fingerprint (or other)) or multi-modal (e.g. fingerprint, facial recognition and voice) approach?

3. Do you use a single (e.g. smart card) or multi-factor (e.g. smart card, pin code and fingerprint) approach?

4. What are the consequences of your biometric system failing?

5. Do you have a contingency / fall-back position? (yes) (no) (Please delete as appropriate)

6. If you answered yes to Qu. 5: what type of contingency do you have?

7. Have you had cause to use the contingency? (yes) (no) (Please delete as appropriate)

8. If you answered yes to Qu. 7: please explain

9. If you use biometric technology: what type of biometric is currently being used?

10. If you are considering using biometric technology: what type are you contemplating?

11. If you do not use biometric technology, please explain why it has not been used or considered: PLEASE GO TO QUESTION 13
12. When was your biometric system introduced ( ) or when is it likely to be introduced ( ) or when was the non-biometric system introduced ( )? (Please indicate with an X as appropriate)

13. What strategies did you ( ) or will you ( ) use to introduce your technology to workplace members? (Please indicate with an X as appropriate)
   a) Consultation [ ]
   b) Organisational Policy [ ]
   c) Other (please specify) [ ]

14. Did you use an organisational strategy for implementation? (yes) (no) (Please delete as appropriate)

15. If you answered yes to Qu. 14: was it:
   A technology acceptance model (TAM) (yes) (no) (Please delete as appropriate)
   Other (Please specify):
16. What do you ( ) would you ( ) consider the main concerns associated with the implementation of biometric access control?

(Please indicate with an X as appropriate)

a) Social Issues [ ]

b) Legal Issues [ ]

c) Ethical Issues [ ]

IF YOU DO NOT USE BIOMETRIC ACCESS CONTROL: GO TO QUESTION 26

17. What is your opinion of biometric technology used for access control?

18. What legislation (if any) do you consider necessary to appropriately use biometric technology in the workplace?

19. Have you had any experience of the following standards and European funded projects relating to the practical management of this technology? (yes) (no)

(Please delete as appropriate)

a) ISO/IEC TR 24714-1:2008 – Biometrics, Jurisdictional and Societal considerations for Commercial Applications and Design of Biometric Systems [ ]
b) EnCore (Ensuring Consent and Revocation)[ ]
c) PV Nets (Privacy Value Networks)[ ]
d) VOME (Visualisation of Other Methods of Protection)[ ]
e) RISE (International Platform devoted to the Ethics of Biometrics and Security Issues)[ ]
f) Other? (please specify)
20. If you answered yes to Qu. 19: how have they been considered / implemented by your organisation?

21. How did workplace members respond to the introduction of biometrics?

(Please indicate as appropriate)

a) Positively – approx. % [ ] for example........

b) Negatively – approx % [ ] for example...........

c) Neutrally – approx % [ ] for example.............

22. What types of particularly positive or negative responses did you experience (if any)?

23. Did you request feedback from workplace members? (yes) (no) (Please delete as appropriate)

24. If you answered yes to Qu. 23: how was this requested and how did you respond to the request?

25. Now that you have the benefit of experience, what changes (if any) would you make to your implementation and / or management strategies for access control to workplace members?
Appendix 4: Biometric Access Control for Workplace Management

STATEMENT OF PURPOSE

To investigate the development of biometric access control systems (primarily relating to fingerprint scanning and facial recognition) in a sample of United Kingdom organisations.

Please be aware that you may decline to answer any of the questions in this interview and you have the right to remain anonymous.

Conducted with WORKPLACE PARTICIPANTS

Name of Organisation:

Date of Interview:

Name of Interviewee:

Job Title / Status:

Email address:

1. What is the background to the security roles of your organisation?

2. What is your perception of access control security since the events of September 11th 2001?

3. What type of Access Control system is used by your organisation / institution?

4. What is the technology used for?
5. When were you introduced to this technology?

6. What strategy did your organisation / institution use to introduce the system to you?

(Please indicate with an X as appropriate)

- Verbal notification [ ]
- Written notification [ ]
- Consultation [ ]
- Organisational / Institutional Policy [ ]
- No specific policy / consultation [ ]

Other (please specify):

7. Were you given the opportunity to raise an objection to this technology?

a) If yes: did you raise an objection?

b) If no: would you have raised an objection if you had been given the opportunity to do so?

c) Briefly explain why you would or would not raise an objection to this technology:

8. Do you use a single (e.g. fingerprint (or other)) or multi-modal (e.g. fingerprint, facial recognition and voice) approach? (Please delete as appropriate)

9. Do you use a single (e.g. smart card) or multi-factor (e.g. smart card, pin code and fingerprint) approach? (Please delete as appropriate)
10. Have you ever been denied access to the biometric system due to a false negative – i.e. not being recognised despite using your authorised biometric data?

11. If you answered yes to Qu. 10: briefly explain what happened and how the problem was resolved:

12. What do you consider to be the main concerns associated with the implementation of biometrics?

   a) Social concerns:

   b) Legal concerns:

   c) Ethical concerns:

13. Are you aware of the legislation protecting your personal data and human rights? (yes) (no) (Please delete as appropriate)

14. If you answered yes to Qu. 13: which legislation do you think provides greatest protection for your rights and why?

15. Was this legislation brought to your attention at the time your organisation introduced the biometric system for access control? (yes) (no) (Please delete as appropriate)
16. Have you been introduced to any of the following standards and European funded projects relating to practical management of this technology? (Please indicate with an X as appropriate)

   a) ISO/IEC TR 24714-1:2008 – Biometrics, Jurisdictional and Societal considerations for Commercial Applications and Design of Biometric Systems [ ]
   b) EnCore (Ensuring Consent and Revocation)[ ]
   c) PV Nets (Privacy Value Networks)[ ]
   d) VOME (Visualisation of Other Methods of Protection)[ ]
   e) RISE (International Platform devoted to the Ethics of Biometrics and Security Issues) [ ]
   f) Other? (please specify)

17. If you answered yes to any of the examples in Qu. 16: which (if any) of these standards were brought to your attention at the time your organisation introduced the biometric system for access control

18. In your experience of biometric technology for access control in your organisation / institution, could any further practical measures have been taken to reduce concerns you have or had about this technology? (yes) (no) (Please delete as appropriate)

19. If you answered yes to Qu. 18: please specify:

20. Do you have any other opinions or perceptions about the use of biometric access control in your organisation / institution? (yes) (no) (Please delete as appropriate)

21. If you answered yes to Qu. 20: please specify:

Many thanks for your co-operation. Your responses are important to the work I am undertaking.
Appendix 5: Analysis of Feedback from Interview Participation and Suggested Best Practice responding to the Social, Legal and Ethical perceptions of Biometric Access Control Management [Case Study A]

Introduction and Rationale
Separate analysis was undertaken of the feedback received from management and workforce representatives and students at the institution. The responses have been summarised below. This summary is followed by contextual reference to elements of “Best Practice” in the area of access control management. This process linked management and personnel responses with “Best Practice” indicators in order for the reader to assess each individually together with the integration of response and practical linkage with “Best Practice.”

Following the reader’s review and feedback, a series of recommendations for “Best Practice”, was compiled, combining academic and professional observations, activities and suggestions towards access control management in compliance with established social, legal and ethical perceptions.

Interview Responses and Analysis
Representation from Management reported that the organisational policy is based on need but, in terms of the strategy adopted to communicate with recipients, reference was made to a concurrent application of signage and fingerprint scanning, with opportunity being provided for objective assessment of the social, legal and ethical impact arising from these systems,

The institution had an appreciation of the practical application of domestic regulations arising from the Data Protection Act 1998 but this did not extend to any formal knowledge of the European Regulations and Standards associated for example, with ISO/IEC/TR 24714-1-2008 (providing guidelines for the stages in the life cycle of the biometric and associated elements of a system (clarifying societal, cultural and ethical
issues related to the use of biometrics for identifying people) or the various European funded projects associated with Access Control Management.

On the question of institutional strategies to respond to workplace and student concerns relating to methods of access control management, there was evidence of explanation and negotiation but emphasis was placed on the compulsory status for implementing access control methods, with Government edict perceived to preclude any practical room for change or flexibility in approach. Irrespective of relative inertia, there were reports of structured and consistent dialogue being undertaken between managers and welfare officers, in an attempt to respond to social concerns. A practical example of this process was cited in which management had engaged in discussions with workforce and student cohorts about the provision of a total biometric package being developed in time, where the provisions of additional (whilst as yet unspecified facilities) had been suggested in conjunction with the maintenance of the traditional database associated with access control. This suggestion was received with caution however, based on concerns expressed about the risk of mismanagement and misuse of data being packaged in the same facility, leading to practical difficulties for control.

In response to practical concerns of this nature, whilst the institution expressed no plans for the immediate introduction of an integrated system, it emphasised its focus on relative assessments of benefit and efficiency for the institution, in which, given the nature of the student cohort, direct links may be forged with United Kingdom Border Agency policies for access control. But this consideration has yet to be officially recognised and, in the event of its implementation, there remains uncertainty about the extent to which staff and students will consider this move to be socially, legally and ethically advantageous.

This scepticism was identified in the perception of some students at the college that whilst security is maintaining its strength throughout educational establishments and public/private organisations, the practicality of implementing a system in which institutions of this nature can practically vet all those gaining access and egress for potential risk factors, is minimal. The potential to negatively affect student attendance
with negative implications for the overall educational experience and ultimately, the
development of success within that institution was expressed. Concern was also raised
about the actual level of security provided by access control systems as opposed to their
perceptions of security, in cases where the application merely recorded attendance,
providing recipients with the opportunity to leave immediately afterwards or providing
opportunities for complaint where students formed large queues to sign in at flash-point
times of the day.

A contrary argument was raised however, witnessed in both management and student
responses to questions of whether they would formally object to the application of
biometric access control management within the institution. In response to this question,
the majority of respondents indicated that, on reflection, they were unlikely to raise any
practical objection, emphasising the relative necessity for security systems to manage
access control in the current environment. But, this attitude was tempered in response to
the question of instances in which the system resulted in “false negative” or “false
positive”, leading to the intermittent need for respondents to provide manual prints,
where the biometric application failed to recognise the presentation of genuine prints.

The question of practical social, legal and / or ethical concerns arising from the
implementation of biometric access control systems at this institution, led to emphasis
on the ethical impact associated with the requirement for students (past the age of
majority) to register attendance, despite the compulsory attendance of students not
forming part of the institutional policy. Whilst on the question of practical social and
legal concerns there was no reference to social issues in this instance, there was general
recognition of the existence and impact of Data Protection and Human Rights
legislation, having been brought to the attention of both workforce and student cohort
upon joining the organisation.

The Concept of “Best Practice”
In the context of this research, “best practice” applies to the process by which
organisations may balance elements of unique features with those it has in common
with other organisations. But it must be appreciated that, whilst best practice may be achieved by replicating procedures traditionally established in other circumstances with other groups of people over a period of time, this phenomenon should not be considered static, but should be considered as being subject to evolution with time. This may lead to the development of “Evolving Practice” rather than “Best Practice”.

**Best Practice Model for Consideration**

The policy considered for practical suggestion in this research process was introduced by the United Kingdom Government Department for Trade and Industry (DTI) and published by the British Standards Institute (BSI) in 1995, as a formal policy for the maintenance of best practice for information security management (Saint-Germain, 2005).


In assessing the appropriate application of this standard to the current research path, its security controls were reviewed in conjunction with the primary investigation undertaken for this research process, following which, a sample of six Controls was selected, for practical application to the current primary study:
Selected Controls for Application to “Best Practice”

1. Risk Assessment and relevant management;
2. Security Policy and management;
3. Human Resources Security – for employees joining, moving and leaving the organisation;
4. Physical and environmental security – protection of facilities;
5. Access Control – management of access rights to physical and technical applications; and

Suggested Best Practice

Please review the following and provide your views as to the practicality of each within your institution.

Having reviewed and analysed the responses from practical interviews conducted with Case Study, a series of “Suggestions for Best Practice” were identified, in the institutional management of access control, in response to issues of social, legal and ethical concern as follows:

1. In response to: There currently being no formal policy adopted to implement signage and fingerprint scanning applications...

   Suggested Best Practice:
   *Introduce a security policy and confirm practical management strategies for its implementation.*
2. **In response to:** There being institutional knowledge relating to domestic legislation but no evidence of knowledge associated with European Regulations and Standards or Funded Projects.

**Suggested Best Practice:**
*Introduce and Implement Information Systems policies to incorporate European standards, laws and regulations (including European funded projects).*

3. **In response to:** Management responses to student concerns involve explanation and an element of negotiation but with institutional perception of Government edict – providing little room for manoeuvre...

**Suggested Best Practice:**
*Introduce a Human Resources Security strategy – for employees joining, moving and leaving the organisation, highlighting the extent of institutional control over access control management.*

4. **In response to:** Management plans to introduce a total biometric package in time, eliciting concerns associated with misuse of data...

**Suggested Best Practice:**
*Undertake an initial Risk Assessment of the proposed procedure and highlight and relevant management strategies in response.*

5. **In response to:** Future Management plans to develop an integrated system for access control management (in conjunction with Border Agency regulations etc.)...
Suggested Best Practice:
*Clarify the Security Policy established to ensure social, legal and ethical compliance with data security and integrity and indicate practical management approaches.*

6. **In response to:** Student perceptions of biometric access control systems having the potential to have a negative effect on both student attendance and the overall student experience at the institution...

Suggested Best Practice:
*Consult with students to introduce a Human Resources Security strategy – to cater for consultation with and advice for those joining, moving and leaving the organisation.*

7. **In response:** Workforce suggestions that opportunities were not presented to raise objections about the implementation of this technology....

Suggested Best Practice:
*There should be Human Resources Security available for employees joining, moving and leaving the organisation.*

8. **In response to:** Perceived lack of opportunity for workforce to raise objections to access control technology...

Suggested Best Practice:
*Implement clear Security Policies containing clear Management methods. In response to:* Reasons for security systems being necessary to manage security...

Suggested Best Practice:
*Risk Assessment and relevant management – to reveal access to relevant physical and technical applications.*
9. **In response to**: questions of both false positive and negative...

   **Suggested Best Practice:**
   *Combination of Risk Assessment and relevant management and Physical and environmental security to protect facilities*

10. **In response to**: the combination of social, legal and ethical concerns....

   **Suggested Best Practice:**
   *Development of Information security policies – incorporating standards, laws and regulations, and*

11. **In response to**: the extent of knowledge of current legislation (Data Protection / Human Rights etc.)

   **Suggested Best Practice:**

**Conclusion**

During the investigation with Case Study A, a series of interviews were conducted with representatives of management, workforce and students to identify the current access control system. The responses were analysed to consider the concept of Best Practice in the development of a biometric access control system to fulfil the social, legal and ethical requirements of management, workforce and student cohort.

The result of the primary investigation and subsequent analysis has been to consider the definition and practical effect of a Best Practice model in the implementation of a biometric access control system for the institution. This has culminated in a series of
practical suggestions to address each of the issues identified from the initial investigation.

Investigation was undertaken into both primary and secondary applications with a view to producing a practical set of suggestions for participants in Case Study A. Suggested indicators of Best Practice were subsequently sent to participants for their consideration, review and feedback. This information formed the basis for a set of practical recommendations to ensure Best Practice towards the implementation of biometric access control within the institution, ultimately having the potential for application across similar institutions of this nature.
Appendix 6: Analysis of Feedback from Interview Participation and Suggested Best Practice responding to the Social, Legal and Ethical perceptions of Biometric Access Control Management [Case Study B]

Introduction and Rationale
Separate analysis of the feedback received from management and workforce representatives was undertaken at this organisation. The responses have been summarised below. This summary is followed by contextual reference to elements of “Best Practice” in the area of access control management. Management and personnel responses have been linked with “Best Practice” indicators in each case.

Following the reader’s review and feedback, a series of recommendations for “Best Practice”, were compiled, combining academic and professional observations, activities and suggestions towards access control management, in compliance with established social, legal and ethical perceptions.

Interview Responses and Analysis
Representation from Management reported that the sensitive nature of the Data Centre has led to physical systems being necessary to ensure security. This is evident by the presence of cameras at specific locations and both internal and external fencing protecting security critical areas. The respondent emphasised that, despite the impact of the terrorist attack in September 2001, there have been no changes in organisational strategy because security has always been regarded as paramount due to the nature of work being undertaken. The primary tasks at the centre relate to the hosting of data and equipment for banks and building societies through to Government and Ministry of Defence (MOD) related material.

Whilst there is no strategic organisational policy for the application of this technology in an access control capacity, the respondent pointed to a series of consultations taking place. They occur during interview processes (at which time appropriate security levels are assessed) and balanced against the various job functions of individual candidates,
towards compiling accurate levels for Security Clearance and Defence Vetting. This approach precludes the need for prescriptive organisational policies, focusing on the practical design and appropriate implementation of specific systems for discrete environments.

The respondent recognised the primary importance of the Data Protection Act among the legal regulations in this area, but he made reference to the nomination of this specific organisation and location, as representing the first such European organisation to recognise and demonstrate compliance with the ISO27001 for the Accreditation of Data Centre Standards with universal recognition whereby access security standards are audited by Lloyds of London.

With the benefit of wide-ranging organisational experience in implementing the biometric security system in question, the respondent reported purely positive perceptions leading to no planned changes beyond the application of new levels of software and the installation of new hardware to maintain efficiency. He focussed on strategies for technology refresh as opposed to replacement.

In relation to workforce respondents, there was no reference to organisational consultation beyond the use of verbal notification. Three of the six respondents in the selected sample, however, acknowledged the use of organisational security policies, with one respondent reporting that the application of this policy had been clarified with her before her access to the building in September 2008.

Conversely, whilst agreeing that biometric technology represents a useful tool in maintaining security in specific areas, one respondent suggested that if the system were to be used in a more diverse way (for example, in monitoring workforce attendance) she would consider this to be an abuse of power. In expressing this view, she referred to the potential for biometric systems to represent “Big Brother” in their association with access control management.
On the question of whether this application had ever resulted in denial of access arising from false negative responses to otherwise authorised members of the workforce, two respondents reported experience of this. In each case, however, the respondents suggested that an acceptable solution had been found to secure access following engagement with the central (on-site) security system.

In instances in which scanning equipment intermittently failed to recognise respondents due to poor background lighting, a resolution was reported by the adjustment of scanner angles or the use of re-scanning. Whilst a solution was found by these procedures, the respondent alluded to having in some instances, to crouch or to stand on tip-toe, in order to gain appropriate recognition and security clearance.

The social perceptions and concerns expressed ranged from security systems leading to guests at the organisation having to be chaperoned, with perceived constraints on the mobility of personnel within the buildings, to those about access to and the security of data retained at the organisation. There were also perceived risks associated with the potential to track and copy personal data acquired and stored within the organisation.

From a broader social perspective, a respondent reported her resistance to the more widespread use of biometric technology, citing its comparative expense and a perception of the risks associated with this technology outweighing its benefits. Justification for this statement stemmed from a perception that in a relatively short space of time, criminal elements would find a means of falsifying identities and illegally gaining access to personal data. This respondent further considered the potential for such systems to become exploitative, in what she considered to be an increasingly authoritarian and governmental regime.

The legal concerns reported ranged from issues associated with data protection in considering who accesses the information recorded by biometric systems and where these details are kept, to those associated with justification for the retention of data. These concerns were tempered however, with reference to training in data protection legislation within the organisation, and the recognition that appeals could be made to
challenge any suggestion of faulty evidence being generated by biometric data. The respondent further suggested that if biometric technology is to be more widely relied on, the whole issue of legal identity and its protection should perhaps be reinforced with further legislative provision.

The ethical considerations ranged from suggestions that organisations may use biometric access control technology to track the movements of employees, to opportunities being provided to discriminate against minority groups in employment. Specific reference was made in this context, to the potential difficulty presented by retina scanning towards members of the workforce who are blind or visually impaired, leading to appropriate contingencies having to be found for them in order to ensure consistency of application and equality of treatment.

Having pursued issues of social, legal and ethical concern raised by the respondents, the interview questions proceeded to link practical perceptions with an appreciation of European funded projects in existence, to consider the practical management of biometric technology for access control within the United Kingdom. Whilst avoiding any suggestion that this should represent an exhaustive list, this question cited a number of examples of projects, ranging from ISO/IEC TR 27414-1-2008 – Biometrics, Jurisdictional and Societal Considerations for Commercial Applications and Design of Biometric Systems; EnCore (Ensuring Consent and Revocation); PVNets (Privacy and Value Networks); VOME (Visualisation of Other Methods of Protection) and RISE (International Platform devoted to the Ethics of Biometric and Security Issues), with no respondents having reported knowledge or recognition any of these projects. This led to the general question of respondents having suggestions for any further practical measures required to reduce the social, legal and ethical concerns cited in response to questions raised in this interview.

One response was made to this question, specifying the need for the organisation to clarify the implementation and application of the biometric system used (in this case, iris scanning technology) as opposed to adopting a strategy in which workforce members were forced to ask specific questions about the practical applications of the
system and its effects. More specifically, this respondent, whilst recognising that questions were addressed by Line Management when they were raised by members of the workforce, expressed continued concern about the possible long-term health implications of biometric scanning technology being associated with the body and more especially, facial features. Despite its generally positive reception, the respondent tempered this with an expression of interest that biometric access control technology should apply in a manner that satisfies workforce assurances of safe data management in which personal rights to informed consent in the acquisition, maintenance and storage of personal data is respected.

The Concept of “Best Practice”

In the context of this research, “best practice” may apply to the process by which organisations may balance elements of unique features with those it has in common with other organisations.

It is important to recognise however, that whilst best practice may be achieved by replicating procedures traditionally established in other circumstances with other groups of people over a period of time, this phenomenon should not be considered static, but should be considered as being subject to evolution with time. This may lead to the development of “Evolving Practice” rather than “Best Practice”.

Best Practice Model for Consideration

The policy considered for practical suggestion in this research process has been previously identified and implemented within the participant organisation. It was introduced by the United Kingdom Government Department for Trade and Industry (DTI) and published by the British Standards Institute (BSI) in 1995, as a formal policy for the maintenance of best practice for information security management (Saint-Germain, 2005).
The initial title of the policy was BS7799, but following consultation between the UK Government and international standards bodies, this Standard was revised and adopted by the International Organisation for Standardisation (ISO) in 2000, to become ISO/IEC (International Electro-technical Commission) 17799: “Information Technology – Code of Practice for Information Security Management.”


Despite the general appreciation of this security system within the participant organisation, the researcher suggested that specific points of reference from the empirical investigation conducted into this research area be applied to individual management strategies towards securing social, legal and ethical responses to the management of access control facilities within this case study. She reviewed the security controls contained in this standard in conjunction with the primary investigation undertaken for this research process, following which, she selected a sample of six Controls as being practically applicable to the current primary study:

**Selected Controls for Application to “Best Practice”**

7. Risk Assessment and relevant management;
8. Security Policy and management;
9. Human Resources Security – for employees joining, moving and leaving the organisation;
10. Physical and environmental security – protection of facilities;
11. Access Control – management of access rights to physical and technical applications; and
12. Information security policies – incorporating standards, laws and regulations.
Suggested Best Practice

*Please review the following and provide your views as to the practicality of each within your institution.*

Having reviewed and analysed the responses from practical interviews conducted with Case Study 3, I identified a series of “Suggestions for Best Practice” in the organisational management of access control, in response to issues of social, legal and ethical concern as follows:

1. *In response to:* Management contention of no current formal policy for introducing biometric access control to the workforce, beyond a series of consultations during interview in which security access levels are assessed.

**Suggested Best Practice:**

*Undertake a review of access control management, focusing on physical and technical applications to ensure compliance with current standards, laws and regulations.*

2. *In response to:* Workforce perceptions of there being no organisational consultation relating to access control management other than verbal notification.

**Suggested Best Practice:**

*Critically assess the current security policy at the organisation in terms of its effective communication to workforce members.*

3. *In response to:* Workforce suggestions that any management plan to extend access control measures to monitor attendance, would be considered an abuse of power.
Suggested Best Practice:

*Ensure that the workforce is fully aware of organisational policies for access control management specifically those associated with physical and environmental security.*

4. **In response to:** Workforce reports of scanning equipment subject to intermittent failure in which organisational resolutions involve changing scanner angles to necessitate change of stance (to crouch position etc.).

Suggested Best Practice:

*Undertake a current risk assessment in areas of physical and environmental security.*

5. **In response to:** Workforce perceptions of lack of mobility within the workplace in cases where guests have to be chaperoned.

Suggested Best Practice:

*This may involve multiple strategies, involving risk assessment and appropriate management responses to current security policies; assurances of human resource security for employees joining the organisation and / or moving within it; the application of express physical and environmental security strategies for access control incorporating access rights in physical to technical applications and the express application of information systems policies incorporating standards, laws and regulations.*

6. **In response to:** Broader social perceptions of technological expense outweighing practical benefit, where criminal elements will find a means of falsifying identification to gain illegal access; together with the equation between function creep and social exploitation.
Suggested Best Practice:
Assure workforce members of risk assessment strategies implemented within the organisation and illustrate methods of associated risk management.

7. In response: Legal concerns emanating from workforce members towards the current application of Data Protection legislation, in the absence of sufficient (perceived) for the rights to store and retain personal data; together with suspicion about the reliability of the current system. This has led to suggestions for the legislation to be reinforced, with further legislation and training.

Suggested Best Practice:
Demonstrate and document the current application of information systems policies incorporating relevant standards, laws and regulations.

8. In response to: Ethical concerns arising from workforce representatives relating to opportunities for employees’ movements to be tracked and for discrimination to arise within minority groups of employees. Specific reference was made to the practise of retina scanning for access control purposes, in which the visually impaired or blind members of the workforce may be subjected to unequal treatment.
Suggested Best Practice:

Undertake regular risk assessment exercises and publish associated risk management strategies.

9. In response to: Workforce perceptions of the practical application of ISO/IEC TR 27414-1-2008 and associated funded projects: with their associated implementation for biometric access control solutions (specifically iris scanning) and subsequent (perceived) long-term health implications.

Suggested Best Practice:

Communicate organisational approaches to assess associated risks and identify organisational methods for practically responding to the risks identified.

10. In response to: Workforce perceptions of the primary roles of communication and consultation, in which assurances are maintained of appropriate data management in the procedure for securing biometric access control. This extended to personal rights being supported with informed consent in the acquisition, maintenance and storage of personal data relating to access control management.

Suggested Best Practice:

The strategies adopted by the organisation in response to workforce perceptions in this instance should be multiple. They should range from the express inclusion of security policies within the working environment and clear strategies to demonstrate management methods in response. This should be combined with specific access control management relating to access rights and access to both physical and
technical applications within the organisation. These strategies should be supported with documented, fully informed information security policies applied by the organisation to ensure compliance with standards, laws and regulations to ensure the dual security of the organisation and its workforce.

Conclusion

During the research process with your organisation [Case Study 3] the researcher has, as you are aware, conducted a series of interviews with yourself (Management) and workforce members at your organisation to identify the current access control system being implemented. She has analysed the responses gained from yourselves and considered the concept of Best Practice in the development of a biometric access control system to fulfil the social, legal and ethical requirements of both management and workforce.

The result of the primary investigation and subsequent analysis has been to consider the definition and practical effect of a Best Practice model in the implementation of a biometric access control system for your organisation, culminating in a series of practical suggestions to address each of the issues identified from the initial investigation.

The researcher has undertaken the above investigation into both primary and secondary applications with a view to producing a practical set of suggestions for you the respondents to (Case Study C). These suggested indicators of Best Practice have been sent to you for your consideration, review and feedback. This information will form the basis for a set of practical recommendations to ensure Best Practice towards the implementation of biometric access control within your organisation and will ultimately have the potential for application across similar institutions of this nature.