Privacy and Security in Ubiquitous Computing:
Service Delivery and Identity in Intelligent Environments

Craig Andrew Chatfield
Bachelor of Science, Bachelor of InfoTech (Hons)

Smart Internet Technology Cooperative Research Centre
School of Information and Communication Technology
Griffith University, Brisbane Australia

Submitted in Fulfilment of the Requirements of the Degree of Doctor of Philosophy

September 2009
Abstract

Ubiquitous computing describes computing technologies that are designed to be embedded in tools and in our environment, providing computational support for user interaction and service delivery. Intelligent environments are context-aware computing environments that deliver services using ubiquitous computing technologies. These environments provide users with services tailored to the users’ preferences and the current state of the environment. The development and implementation of these environments is challenging due to their potential ability to gather information on the environment’s occupants and context. The information collection, when combined with advanced data-mining techniques, has unprecedented potential to invade users’ privacy. The invasion of privacy is a significant concern to users, and must be addressed before intelligent environments can gain widespread acceptance.

The use of ubiquitous computing technologies also poses unique challenges for service delivery and network security. By definition, ubiquitous computing describes computing that has faded into the background, allowing users to use the services and technologies as easily as they would more tangible physical objects. This integration into our world raises the question that if a service is inconspicuous enough to blend into the background, how can we allow users to identify previously unused services? Information security within intelligent environments is complicated by the physical availability of much of the environment’s hardware (which leaves it vulnerable to being tampered with). These privacy and security concerns raise the need for a ubiquitous computing infrastructure that will allow private interaction and the effective delivery of personalised and identity-restricted services.

Owing to the large variety of services they could provide, it has been suggested that intelligent environments will one day cover most of our daily lives (for example our homes, offices, public transport networks or shopping centres). This requires a common approach be taken to users’ interaction with intelligent environments, and suggests a shared infrastructure will be required to support users’ interactions with different environments. User privacy requirements necessitate that this infrastructure be independently operated from the intelligent environments (and its service providers). Further privacy and interaction requirements highlight the need for user-controlled identity management structures and anonymous environmental interaction.

In order to achieve the goal of safe and secure ubiquitous computing support, the dissertation will examine the user privacy and security requirements of an intelligent environment architecture. The primary research question for the dissertation is:

- What type of architecture is required to ensure user privacy and information security during service delivery within intelligent environments?
In answering this research question, this research examines the impacts of interacting with intelligent environments upon a user’s privacy, and the interaction and information security requirements for users interacting with multiple, potentially malicious environments. Activity Theory, Critical Heuristics and User Studies are used to develop the dissertation’s understanding of users’ perceptions of privacy and intelligent environment service delivery. This is used to develop a model of the user interaction with multiple intelligent environments that the architecture will need to support.

The user surveys and field studies carried out have revealed a great deal about users’ perceptions of privacy and information sharing. These findings include the personal nature of their mobile computing devices, users’ desire for effective and digestible feedback on information-sharing events and service delivery, and the need for intelligent environments to respect the same privacy protections that users have in the real world.

Design science is utilised to iteratively develop our architectural requirements, which are then validated by further user studies. This development also allows the security of user information within the architecture to be evaluated. The results from these research activities provide us with requirements for ideal user interaction with intelligent environments. These requirements are used to develop an architecture that can provide a private, secure and scalable ubiquitous computing infrastructure that could be used to provide a pervasive service infrastructure to users wherever they are.

The Secure Privacy Aware Communication Environment (SPACE) architecture is presented and used to integrate existing methods of privacy protection, identity management, service delivery and ubiquitous computing security into a ubiquitous computing infrastructure. Included in the SPACE architecture are Identity Brokers, to allow independent verification of a user’s identity (for service delivery), and environmental structures and safeguards that allow users anonymous interaction with the environment and its inhabitants. This infrastructure, and its supporting global identity management structures, allows private and secure interaction with any intelligent environment service.

This research evaluates the SPACE architecture and identifies extensions to the architecture to further improve user privacy, information security and effective service interaction. It also investigates the requirements for any ubiquitous computing infrastructure that seeks to support users’ interaction across multiple intelligent environments, and provides suggestions on the environmental structures that are required to support service delivery and user privacy. The implementation of these supporting structures (such as the user’s personal domain and the different types of identity management and verification providers) will reduce the considerable concerns users have when interacting with these types of environments. In doing so, this research provides a valuable first step towards making a global ubiquitous computing infrastructure possible, and provides a useful framework for intelligent environment development.
Statement of Originality

This work has not previously been submitted for a degree or diploma in any university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made within the dissertation itself.

Craig Chatfield
September 2009

Acknowledgements

This research was conducted under the supervision of Dr. René Hexel and Dr. Liisa von Hellens. Additional research was conducted in conjunction with Dr. Judy Kay, Dr. Bob Kummerfeld and David J. Carmichael from the Smart Internet Technology Cooperative Research Centre and the University of Sydney, and with Dr. Jonna Häkkilä from the University of Oulu in Finland. Many thanks to all these professional researchers without whose support this research would not have been possible.

This research was conducted with scholarship support from Griffith University and the Smart Internet Technology Cooperative Research Centre. Heartfelt thanks are extended to all members of these organisations who have assisted me during my candidature.

Dedication

This research is dedicated to my parents, Ken and Gloria Chatfield, and to my beautiful future wife Rebecca Mihailovic. I finally did it! Thanks for helping me get here.
# Glossary of Terms

<table>
<thead>
<tr>
<th>Referenced Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Broker</td>
<td>Independent third party that can provide identity authentication for user identity management and service delivery.</td>
</tr>
<tr>
<td>Identity Manager</td>
<td>Blind information request router that connects a third party to a user’s personal domain without revealing their identity or the personal domain's address.</td>
</tr>
<tr>
<td>Intelligent Environments</td>
<td>Ubiquitous Computing adorned environments that monitor their context and provide services to users based upon that context and users’ personal preferences.</td>
</tr>
<tr>
<td>Personal Domain</td>
<td>User Controlled online spaces that can act as a proxy for the user providing user information and managing identity structures.</td>
</tr>
<tr>
<td>Service Provider</td>
<td>An entity that provides a service to users within an intelligent environment.</td>
</tr>
<tr>
<td>Smart Environments</td>
<td>See Intelligent Environments.</td>
</tr>
<tr>
<td>Third Places</td>
<td>Community spaces outside work and the home that provide socialising space for members of the community (for example parks, coffee shops or libraries).</td>
</tr>
<tr>
<td>Ubiquitous Computing (Ubicomp)</td>
<td>Computing technologies embedded in everyday objects to provide novel services and new interaction techniques.</td>
</tr>
<tr>
<td>User Register</td>
<td>Software on a user's mobile computing device for managing user identity and service delivery.</td>
</tr>
</tbody>
</table>
# Table of Contents

Abstract ................................................................................................................. 2
Statement of Originality .......................................................................................... iv
Acknowledgements .................................................................................................. iv
Dedication .................................................................................................................. iv
Glossary of Terms .................................................................................................... v

Chapter One: Introduction ....................................................................................... 1
  1.1 Overview ............................................................................................................ 1
  1.2 Research Contributions ..................................................................................... 4
  1.3 Research Design ................................................................................................ 6
  1.4 Research Publications ...................................................................................... 7
  1.5 Dissertation Outline ......................................................................................... 8

Chapter Two: Background Literature ...................................................................... 10
  2.1 Introduction ......................................................................................................... 10
  2.2 The Digital Society ............................................................................................ 10
    2.2.1 Distributed and Mobile Computing ............................................................. 12
    2.2.2 Ubiquitous Computing .................................................................................. 13
      2.2.2.1 Ubiquitous Computing Technologies .................................................. 14
      2.2.2.2 Ubiquitous Computing Environments .................................................. 15
    2.2.3 Digital Communities .................................................................................... 15
    2.2.4 Summary and Conclusions .......................................................................... 18
  2.3 Intelligent Environments .................................................................................... 19
    2.3.1 Intelligent Environment Examples ............................................................... 21
    2.3.2 Intelligent Environment Architectures .......................................................... 24
      2.3.2.1 Merino Scalable Intelligent Environment Architecture ......................... 25
      2.3.2.2 Framework for Intelligent Instrumented Environments ....................... 26
      2.3.2.3 Gaia OS ................................................................................................ 27
      2.3.2.4 MyPlace Intelligent Environment ......................................................... 28
      2.3.2.5 Personal Server ...................................................................................... 30
      2.3.2.6 Privacy Sensing Ubiquitous Computing ................................................ 32
      2.3.2.7 iCrafter Service Framework .................................................................. 33
    2.3.3 Context Awareness ....................................................................................... 33
    2.3.4 Knowledge Representation ............................................................................ 35
    2.3.5 Personalisation .............................................................................................. 39
    2.3.6 Service Discovery .......................................................................................... 41
      2.3.6.1 Service Oriented Computing .................................................................. 42
      2.3.6.2 Ubiquitous Computing Services ............................................................... 43
    2.3.7 Summary and Conclusions .......................................................................... 44
  2.4 Privacy ................................................................................................................. 45
    2.4.1 Privacy Regulation ....................................................................................... 51
    2.4.2 Privacy Design Strategies ............................................................................. 53
3.5.3 Design Science ............................................................................................. 118
   3.5.3.1 Research Guidelines.............................................................................. 120
   3.5.3.2 Strengths and Weaknesses.................................................................. 122
   3.5.3.3 Summary.............................................................................................. 123
3.5.4 Field Studies ................................................................................................. 123
3.5.5 Survey Research ........................................................................................... 125

3.6 Research Design............................................................................................... 127
   3.6.1 User Perceptions of Information Sharing......................................................... 128
   3.6.2 Personalisation in Intelligent Environments..................................................... 129
   3.6.3 Initial Intelligent Environment Architecture Development............................. 130
   3.6.4 User Evaluation of Initial Intelligent Environment ............................................ 131
   3.6.5 Development of Ubicomp Infrastructure Requirements.................................. 132
   3.6.6 Development of Final Intelligent Environment Architecture.......................... 132
   3.6.7 Evaluation of Final Intelligent Environment Architecture.............................. 133

3.7 Fit of Research Method.................................................................................... 134
3.8 Summary and Conclusions ............................................................................. 135

Chapter Four: Preliminary Investigations into Privacy in Intelligent Environments.............. 136
4.1 Introduction ...................................................................................................... 136
4.2 User Perceptions of Information Sharing............................................................ 136
   4.2.1 User Study Description.................................................................................. 136
   4.2.2 User Study Results........................................................................................ 137
   4.2.3 Discussion and Design Conclusions ................................................................ 142
4.3 Personalisation in Intelligent Environments........................................................ 144
   4.3.1 Intelligent Environment Usage Scenario....................................................... 144
   4.3.2 User Interactions with the Intelligent Environment.......................................... 145
   4.3.3 Discussion and Design Conclusions ................................................................ 147
4.4 Initial Intelligent Environment Architecture.................................................... 148
   4.4.1 Privacy-Aware Intelligent Environment Architecture......................................... 149
   4.4.2 Discussion and Design Conclusions ................................................................ 152
4.5 User Studies of Initial Architecture.................................................................... 153
   4.5.1 User Study Description.................................................................................. 154
   4.5.2 User Study Results........................................................................................ 156
   4.5.3 Discussion and Design Conclusions ................................................................ 157
4.6 Summary and Conclusions ............................................................................... 158

Chapter Five: Privacy Requirements for Ubiquitous Computing Systems......................... 160
5.1 Introduction ...................................................................................................... 160
5.2 Ubiquitous Computing Infrastructure .................................................................. 160
   5.2.1 Digital Communities..................................................................................... 161
      5.2.1.1 Privacy within Ubiquitous Computing Environments............................. 162
      5.2.1.2 Interaction Design Requirements......................................................... 163
      5.2.1.3 Community Interaction....................................................................... 164
5.2.1.4 Usage Scenario ................................................................. 165
5.2.1.5 Discussion and Design Conclusions ................................. 167
5.2.2 Ubiquitous Computing Services ........................................... 168
5.2.3 Identity Management .......................................................... 170
5.2.4 User Interaction ................................................................. 172
5.2.4.1 Intelligent Environment Interfaces ................................. 174
5.2.5 User Information Storage .................................................. 175
5.2.5.1 Securing Interaction Information ................................. 177
5.2.6 Design Conclusions ............................................................ 178

5.3 Intelligent Environment Design ............................................. 179
5.3.1 Information Flow ............................................................... 182
5.3.2 Identity Management .......................................................... 184
5.3.3 Information Storage ............................................................ 187
5.3.4 Design Conclusions ............................................................ 189

5.4 Summary and Conclusions .................................................... 189

Chapter Six: A Solution for Privacy in Ubiquitous Computing ....... 191

6.1 Introduction .............................................................................. 191

6.2 SPACE Architecture .............................................................. 191
6.2.1 User Mobile Device ............................................................ 194
6.2.1.1 Persona Manager ............................................................ 195
6.2.1.2 User Manager ............................................................... 197
6.2.1.3 Service Manager ........................................................... 198
6.2.1.4 Privacy Threats and Analysis ........................................ 199
6.2.2 User Register ................................................................. 200
6.2.2.1 User Register ............................................................... 201
6.2.2.2 User Details Database .................................................... 203
6.2.2.3 User Information Requester .......................................... 204
6.2.2.4 Privacy Threats and Analysis ........................................ 206
6.2.3 Identity Manager .............................................................. 206
6.2.3.1 Identity Manager Connection ........................................ 207
6.2.3.2 Persona Requester ........................................................ 208
6.2.3.3 ID Management Database ............................................. 208
6.2.3.4 Privacy Threats and Analysis ........................................ 209
6.2.4 Personal Domain .............................................................. 209
6.2.4.1 Privacy Manager ........................................................... 210
6.2.4.2 Persona Database .......................................................... 211
6.2.4.3 Privacy Threats and Analysis ........................................ 212
6.2.5 Service Provider ............................................................... 213
6.2.5.1 Service Beacon .............................................................. 215
6.2.5.2 Service Provider ............................................................ 216
6.2.5.3 Authorisation Entity ....................................................... 217
6.2.5.4 Service Database .......................................................... 218
6.2.5.5 Privacy Threats and Analysis ........................................ 219
6.2.6 Information Service Provider ............................................. 221
6.2.6.1 Service Connection ........................................................ 222
| 6.2.6.2 | Templates Database | 223 |
| 6.2.6.3 | Identity Confirmation Entity | 224 |
| 6.2.6.4 | Services Database | 224 |
| 6.2.6.5 | Privacy Threats and Analysis | 224 |
| 6.2.7 | Identity Broker | 225 |
| 6.2.7.1 | Broker Connection | 225 |
| 6.2.7.2 | Broker IDs Database | 226 |
| 6.2.7.3 | Identity Confirmation Authority | 226 |
| 6.2.7.4 | Privacy Threats and Analysis | 227 |

| 6.3 | Prototyping of SPACE Compliant Infrastructure | 228 |
| 6.3.1 | Design Discussion | 228 |
| 6.3.2 | Findings and Analysis | 230 |

| 6.4 | Intelligent Environment Design Requirements | 231 |
| 6.4.1 | Required Ubiquitous Computing Infrastructure Evaluations | 231 |
| 6.4.1.1 | Identity Management | 232 |
| 6.4.1.2 | Information Security | 233 |
| 6.4.2 | Evaluation User Study | 234 |
| 6.4.2.1 | User Study Description | 235 |
| 6.4.2.2 | User Study Results | 235 |
| 6.4.2.3 | Design Implications | 239 |
| 6.4.3 | Summary and Conclusions | 241 |

| 6.5 | SPACE Architecture Extensions | 242 |
| 6.5.1 | Information Tagging | 242 |
| 6.5.2 | User Selected Pseudonyms | 243 |
| 6.5.2.1 | Interaction Example | 244 |
| 6.5.2.2 | System Description | 244 |
| 6.5.3 | Trust and Reputation Systems | 246 |

| 6.6 | Summary and Conclusions | 248 |

Chapter Seven: The Application of SPACE to Achieve Privacy in Ubiquitous Computing | 249 |

| 7.1 | Introduction | 249 |
| 7.2 | Intelligent Environment Architecture | 249 |
| 7.2.1 | User Register | 252 |
| 7.2.2 | User Interaction and Personalisation | 253 |
| 7.2.3 | Identity Brokering | 255 |
| 7.2.4 | Services | 256 |
| 7.2.5 | Information Collection | 258 |
| 7.2.6 | Intelligent Environment Comparisons | 259 |

| 7.3 | Developing Intelligent Environments | 261 |
| 7.3.1 | Ubiquitous Computing Infrastructure | 261 |
| 7.3.2 | Community Connectedness | 263 |
| 7.3.3 | User Education and Interaction Support | 264 |

| 7.4 | Summary and Conclusions | 266 |
Chapter Eight: Conclusions

8.1 Introduction

8.2 Contribution and Results

8.2.1 Privacy and Security in Ubiquitous Computing

8.2.2 Intelligent Environment Architecture

8.2.3 Ubiquitous Computing Infrastructure

8.2.4 Limitations of Research

8.3 Future Research

8.3.1 The Disappearing Computer

8.3.2 Social Integration and Development

8.3.3 Community Integration of Intelligent Environments

8.3.4 Intelligent Agents

8.3.5 Biometrics

8.4 Outlook for Ubiquitous Computing

References

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>267</td>
</tr>
<tr>
<td>268</td>
</tr>
<tr>
<td>268</td>
</tr>
<tr>
<td>270</td>
</tr>
<tr>
<td>271</td>
</tr>
<tr>
<td>272</td>
</tr>
<tr>
<td>274</td>
</tr>
<tr>
<td>274</td>
</tr>
<tr>
<td>275</td>
</tr>
<tr>
<td>276</td>
</tr>
<tr>
<td>277</td>
</tr>
<tr>
<td>278</td>
</tr>
<tr>
<td>279</td>
</tr>
<tr>
<td>281</td>
</tr>
</tbody>
</table>
## Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Merino Abstraction of an Intelligent Environment (Kummerfeld et al., 2003)</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>MyPlace Architecture (Chatfield et al., 2005)</td>
<td>29</td>
</tr>
<tr>
<td>3</td>
<td>MyPlace World Model Example (Chatfield et al., 2005)</td>
<td>30</td>
</tr>
<tr>
<td>4</td>
<td>Semantic Network Representation (Peters &amp; Shrobe, 2002)</td>
<td>36</td>
</tr>
<tr>
<td>5</td>
<td>Activity Theory model (Kuutti, 1999)</td>
<td>112</td>
</tr>
<tr>
<td>6</td>
<td>Research Activities Relationship Diagram</td>
<td>128</td>
</tr>
<tr>
<td>7</td>
<td>Secure Intelligent Environment Architecture</td>
<td>145</td>
</tr>
<tr>
<td>8</td>
<td>Initial Intelligent Environment Architecture</td>
<td>150</td>
</tr>
<tr>
<td>9</td>
<td>MyPlace Visualisation Server Screenshot</td>
<td>155</td>
</tr>
<tr>
<td>10</td>
<td>'Local Area' User Interface Screen</td>
<td>165</td>
</tr>
<tr>
<td>11</td>
<td>'Services' User Interface Screen</td>
<td>166</td>
</tr>
<tr>
<td>12</td>
<td>Secure Privacy Aware Communication Environment Architecture</td>
<td>192</td>
</tr>
<tr>
<td>13</td>
<td>SPACE Architecture Technical Description</td>
<td>193</td>
</tr>
<tr>
<td>14</td>
<td>Sample Intelligent Environment Location Tag</td>
<td>202</td>
</tr>
<tr>
<td>15</td>
<td>User Details Database</td>
<td>203</td>
</tr>
<tr>
<td>16</td>
<td>ID Management Database</td>
<td>208</td>
</tr>
<tr>
<td>17</td>
<td>Personal Domain’s Persona Database</td>
<td>212</td>
</tr>
<tr>
<td>18</td>
<td>Sample Service Interface Tags</td>
<td>215</td>
</tr>
<tr>
<td>19</td>
<td>Services Database</td>
<td>219</td>
</tr>
<tr>
<td>20</td>
<td>Template Database</td>
<td>223</td>
</tr>
<tr>
<td>21</td>
<td>Services Database</td>
<td>224</td>
</tr>
<tr>
<td>22</td>
<td>Broker IDs Database</td>
<td>226</td>
</tr>
<tr>
<td>23</td>
<td>User Study Intelligent Environment Interface</td>
<td>236</td>
</tr>
<tr>
<td>24</td>
<td>Example User Pseudonyms Interfaces</td>
<td>237</td>
</tr>
<tr>
<td>25</td>
<td>Example Service using ‘Secure User Template’</td>
<td>239</td>
</tr>
<tr>
<td>26</td>
<td>SPACE Architecture with Reputation Service</td>
<td>247</td>
</tr>
<tr>
<td>27</td>
<td>Reputation Services in the User and Service Manager Interfaces</td>
<td>248</td>
</tr>
</tbody>
</table>
List of Tables

Table 1: Research Outcomes and Contributing Sub-Questions ................. 103
Table 2: Research Paradigms ................................................................. 104
Table 3: Research Assumptions relating to an Critical Approach ............ 107
Table 4: Ontological Assumptions ......................................................... 107
Table 5: Epistemological Assumptions .................................................. 108
Table 6: Research Methods ................................................................. 109
Table 7: Ethical Assumptions ............................................................... 110
Table 8: Boundary Justification Critique .............................................. 117
Table 9: Research Activities ............................................................... 128
Table 10: Influences on Participants Sharing Personal Information ......... 138
Table 11: Information Sharing Likeliness For Different Influence Factors .. 138
Table 12: Different User Types and Results for Information Sharing ....... 140
Table 13: Examples of Intelligent Environment Services ....................... 170
Table 14: Information Storage within an Intelligent Environment .......... 177
Table 15: Information Storage in Intelligent Environments ................. 188
Table 16: Desired Intelligent Environment Interface Feedback .............. 238
Chapter One: Introduction

1.1 Overview

The dream of ubiquitous computing environments, as set out by Mark Weiser (Weiser, 1991; 1993), is the support of everyday activities with embedded computation in the environment. This allows the exchange of information between components, environmental services and users which could lead to novel and interactive information sharing and reactive services. But this invisible exchange of information poses enormous user privacy and information security concerns, including how personal information can be user-controlled (private), secure and available when moving between multiple ubiquitous computing environments. Examples of this type of architecture can be found in the media and popular science fiction (see below).

The movie *Minority Report* (Dick & Frank, 2002), set in 2054, describes a world similar to today, but with intelligent environments covering transport, shopping centres and workplace environments. These environments have the ability to track users’ movements, through biometric scanners, and to provide users with personalised services, such as remembering what they have previously bought from a store. A user can walk between different intelligent environments without losing access to their personal information. This seamless integration of multiple intelligent environments gives us an idea of what interaction capabilities these environments require.

Other authors have described similar environments in which information is available anywhere as an environment, either as an immersive computer ‘Matrix’ to be plugged into (Gibson, 1984; Wachowski & Wachowski, 1999), or as an invisible ‘datasphere’ (Simmons, 2003) that covers our physical environments, similar to the *Minority Report* example. These fictional instantiations of the Internet pervading all areas of our physical lives are (predominantly) believable next steps in our access to information. Current Internet access developments are moving through the city-wide wireless networks stage and in some cases now cover entire countries. The dissertation will consider how users can interact with similar computing environments and services in a private and secure way.

Ubiquitous Computing, alternatively known as Pervasive Computing or Disappearing Computing, seeks to change the way computers are used, from being the focus of our attention to simply being tools that are used to accomplish everyday tasks (Weiser, 1993). Computing devices are becoming smaller, more specialised and even embedded in common everyday tools, such as communication devices in ski clothing or pens that remember what they have written. Research into ubiquitous computing varies from the development of specific interaction tools and user interfaces to the construction of complete systems that gather environmental information and provide services to users. Interactive environments that provide services to
users using ubiquitous computing technologies are called ‘Intelligent Environments’ (Coen, 1998).

To ensure consistency throughout the dissertation, the following definitions of ‘architecture’ and ‘infrastructure’ are provided. An architecture is an abstract model of constituents of a system and their inter-relationships, while an infrastructure is underlying elements and processes necessary to enable a complex set of functions to be performed. The system or environment’s infrastructure could describe the underlying transmission and communication protocols, or it could describe sub-systems that are used to provide more complex services or interactions. This dissertation will begin by developing an intelligent environment architecture, and will use this architecture to identify the requirements for the ubiquitous computing infrastructure that provides support for multiple intelligent environments. These definitions are explained in more detail in section 2.3.

Intelligent environments utilise novel methods of sharing and collecting information and are often designed to be aware of the context of their usage (Dey, 2001; Lederer, Dey & Mankoff, 2002). This awareness allows them to detect what is happening in the environment and to tailor their services accordingly. Products such as smart houses, intelligent work spaces and environment-specific information providers have been developed to provide services to existing user environments. In investigating the use of intelligent environments, the dissertation will examine the following research question:

**What type of architecture is required to ensure user privacy and information security during service delivery within intelligent environments?**

This research question has many parts, each of which must be answered before a complete understanding of user interaction within intelligent environments can be reached. Firstly the dissertation must consider the types of interactions users want with intelligent environments and the impact of these interactions on a user’s privacy. Central to the question of user privacy is the security structures required to secure user information and communications whilst interacting with an environment and its users. This question is complicated by the physically accessible nature of many ubiquitous computing components and by the often passive nature of the communications that can happen without the user’s knowledge.

The dissertation will also consider the implied question of how users interact with multiple intelligent environments. The implication that intelligent environments will cover many (if not all) areas of our lives in the near future (Lahlou, Langheinrich & Röcker, 2005) compels the dissertation to consider the structures that are required in this view of a ubiquitous computing-supported world. User interaction within these environments will be studied by means of user surveys and field experiments. Findings from these studies will identify the structures required to support such interactions, and will validate suggested privacy theories and intelligent environment architectures (described in chapter two). The dissertation’s primary research question is deconstructed into sub-questions in section 3.2.
The sheer number of intelligent environment prototypes either developed or currently under development ensures there is no standard interface or interaction method. Similarly there is no standard method of collecting, storing and distributing information within ubiquitous computing environments. This is problematic if we are striving to allow users to interact with many different intelligent environments overlapping across their everyday environments, for example our offices, homes or transport networks. This lack of consistency also causes concern for users worried about the collection and redistribution of their personal information or activities.

Many intelligent environments passively share information with users’ mobile devices to provide contextual or personalised services, usually without the explicit consent of the device’s owner. This is primarily for usability reasons, to avoid requiring users to constantly manage their interaction with the environment, effectively adhering to the minimal cognitive burden design goals of ubiquitous computing technologies. However, this invisible use of information is a cause of concern for many users with regard to the potential use of the information. Langheinrich (2001) identified users’ unwillingness to trust ubiquitous computing systems as the major impediment to their acceptance. The need to incorporate user privacy concerns into these systems has led to many novel and varied ways of seeking to ensure privacy in these systems. Whilst there has been some work identifying privacy design guidelines for ubiquitous computing systems (Lahlou & Jegou, 2003), there has yet to be a systematic development of an architecture to safeguard user privacy across multiple intelligent environments.

The unique nature of intelligent environments also raises security concerns that must be addressed if user privacy is ever to be guaranteed. The presence of often physically accessible hardware and the wireless transmission of information using relatively simple devices bring their own security challenges. The architecture for these environments must therefore have adequate security protections, and users must have confidence in their security before they are willing to use the environments. To this end adequate security must be provided if user privacy is to be maintained during interactions within an intelligent environment.

This research develops the Secure Privacy Aware Communication Environment (SPACE) architecture that could be used to develop scalable, private and secure intelligent environments. This reference architecture provides intelligent environment researchers and developers with a reference architecture that can be used, along with existing research on privacy approaches and security mechanisms, to control the release of user information and prevent breaches of user privacy and system security. This in turn allows the development of a ubiquitous computing infrastructure that can become a supporting infrastructure that can provide services to users across the different environments in which they live and work. This research also considers user involvement and the role of user education in establishing trust with intelligent environments developed using the SPACE architecture.
To assist in the development of the SPACE architecture, the dissertation develops a model of the infrastructure required to support user interaction with ubiquitous computing environments. Developed from existing theory and the results from user studies, this infrastructure provides the same interaction capabilities (especially with respect to identity management and anonymous interaction) that users enjoy in the real world. The statement of infrastructure requirements will be of further use to researchers and developers of intelligent environments, and will provide guidance for future developments based upon the SPACE architecture. The requirements, along with the user studies results, are included in the SPACE architecture as the design was iteratively improved to provide adequate interaction capabilities, user privacy and information security.

### 1.2 Research Contributions

This research addresses the inherent privacy problems associated with users interacting with ubiquitous computing environments and their pervasive and invisible information sensing and collection capabilities. As effective privacy (in modern networks) is impossible without adequate security, the dissertation examines the duality of privacy and security within these environments. In particular this research explores how users perceive privacy in ubiquitous computing environments, and what intelligent environment architecture can support users’ privacy preferences and allow services to be delivered securely. This section considers the theoretical contributions that this research makes to both the theory surrounding intelligent environments and the practical contributions that result from the development of the SPACE architecture.

The major contributions to theory provided by the dissertation are threefold. Firstly the background literature review presented in chapter two examines the existing ubiquitous computing research (and development) that consider user privacy, information storage and technical security. This review highlights areas of research that require more investigation and draws conclusions about required attributes of user privacy and security aware intelligent environments. Conclusions from this chapter are integrated into a holistic picture of user privacy and ubiquitous computing design (including design strategies to reduce threats to users’ privacy and their information’s security).

The second theoretical contribution builds on conclusions from the literature review, along with user studies and an investigation into the technical realities of creating intelligent environments, and develops design goals for developing a ubiquitous computing infrastructure. This infrastructure (described in chapter five) demonstrates the required environmental structures that allow users the kind of interactions within intelligent environments that they enjoy in the real world. This includes the required methods of identity management, the impact of user interaction on their privacy and information security, and the types of ubiquitous computing services that could potentially be integrated into users’ everyday environments.
The final theoretical contribution is also this thesis’ main contribution to practice. The SPACE architecture (described in chapter six) provides a solution for maintaining users’ privacy and managing service interaction within intelligent environments. Of particular interest will be the concept of a global ubiquitous computing infrastructure, supported by the scalable SPACE intelligent environments overlapping physical environments as required. This model describes the environmental structures (like identity brokers) that provide cohesion and standardised user interaction between intelligent environments. The integration of this ubiquitous computing infrastructure into the real world will be of great interest, as will its ability to provide the connectedness that is missing from communities in many modern western cities. Expected outcomes of this research are explored further in section 3.2.

The SPACE architecture provides developers with a blueprint for an intelligent environment with built-in privacy and security safeguards. This enables developers to either create the SPACE architecture as designed, or provides guidance on fundamental user privacy designs that can empower users with control of their information within intelligent environments. The SPACE architecture also sets out required security measures that should be in place in all intelligent environments. This will be of great interest to intelligent environment developers, even when they adopt different service interaction and identity verification methods.

The SPACE architecture developed in the dissertation focuses closely on the available user interaction and the impact of information sharing upon users’ privacy. Information security is provided by secure communication channels (using encryption and key distribution architectures), obfuscating identifiable user details (particularly from mobile devices used to interact with the architecture) and by signing an environment’s components to prevent spoofing and similar attacks. Limitations in the scope of the dissertation prevented the implementation of all components of the SPACE architecture. When these components were not implemented into the SPACE architecture prototypes, it was because they were not integral to the architecture’s evaluation, had already been successfully implemented in a similar setting and are explicitly listed as not implemented in section 6.3.1.

The other main contribution the dissertation makes to practice is the exploration of additional features, described in section 6.5, which could greatly improve the SPACE architecture’s security, privacy and usability. Practical extensions to the SPACE architecture include the use of metadata tags to secure information and the role User Selected Pseudonyms and Trust & Reputation systems can have upon users’ interactions with intelligent environments. Further improvements that require more research to be integrated with the SPACE architecture are described in section 8.3. These include the impacts of the future directions in ubiquitous computing research, methods of integrating the SPACE architecture into communities, the use of intelligent agents in managing users’ interactions and the role of biometric devices in ubiquitous computing environment interaction and information security. These features were outside of the scope of the dissertation and have been included as future work to extend the SPACE architecture’s design.
Further theoretical contributions include: analysis of the ability of ubiquitous computing environments to support community connectedness through user services; the validation of specific theories on user privacy within intelligent environments; and the examination of using Activity Theory and Design Science methodologies (see section 1.3 and 3.5) for this type of research. Further practical contributions include the collection and analysis of security research to aid developers in making general security design decisions, and the analysis of existing intelligent environments and their privacy and security shortcomings.

1.3 Research Design

Research assumptions were developed as part of designing the correct research approach for the dissertation. These assumptions include the (Ontological) assumptions made about the phenomenon to be investigated, and the (Epistemological) assumptions made about the world and how it can be investigated. Further research assumptions (Methodological) describe the appropriateness of using different research techniques on the given problem, and the ethical assumptions that describe the purpose and goals of the dissertation.

These research assumptions helped identify the suitability of the selected critical research paradigm. The selected paradigm in turn helped shape the view of the problem under investigation and consequently the research assumptions listed above. The research assumptions also guided the researcher on the appropriateness of various research methodologies and led to the selection of the research methods found in the dissertation. The research assumptions of the dissertation are discussed in detail in section 3.4.

This research examines how intelligent environments can fit seamlessly into users’ lives and provide them with contextually aware, environmentally specific services. Activity Theory (Engeström, 1987; Leont’ev, 1978; Vygotsky, 1978) is used to examine the interaction between users and the environment, and identifies the core requirements (or interaction goals) that supplement the development of intelligent environment prototypes. The use of Activity Theory allows the dissertation to consider what it is trying to achieve beyond the current technical limitations of this field, and the laboratory experiments will allow a critical evaluation of the value of our architecture’s design. Critical Heuristics (Ulrich, 1987) is utilised to support Activity Theory in the evaluation of what aspects of the ubiquitous computing space should be examined. These research methods are supported by the Design Science paradigm.

The Design Science paradigm (March & Smith, 1995; Simon, 1981) investigates the privacy and security design requirements of intelligent environment architecture through the iterative development of an intelligent environment. The Design Science paradigm seeks to extend the boundaries of human and organisational capabilities by creating new and innovative artefacts (Hevner, March, Park and Ram, 2004). Using the Design Science paradigm allows us to understand the problem domain of the dissertation and develop a solution by creating and evaluating the designed artefact, in this case the intelligent environment architecture. Developed prototypes are
An initial investigation of users' perceptions of privacy and interaction with ubiquitous computing environments was conducted alongside an investigation of mobile phone usage and perceptions of privacy using mobile devices. The questionnaires and user interviews that made up this research were delivered in conjunction with Dr. Jonna Häkkilä and were previously published in (Chatfield & Häkkilä, 2004; Häkkilä & Chatfield, 2005). In this user study the questions investigating user perceptions on information sharing within...
Chapter One: Introduction

intelligent environments, primarily those reported in section 4.2 and in (Chatfield & Häkkilä, 2004), were designed by the author of the dissertation, and the questions regarding the users’ ownership of mobile phones, reported in (Häkkilä & Chatfield, 2005), were designed by Dr. Jonna Häkkilä. Both researchers were involved in the execution of this research.

Further initial investigation into this research area examined personalisation of a user’s interaction with an intelligent environment. It examines how the user interface can be personalised, the privacy and security implications of the personalisation and the effect of this design on the overarching intelligent environment architecture. This research, described in section 4.3, was originally published in the Ubicomp 2004 Privacy Workshop (Chatfield, Carmichael, Hexel, Kay and Kummerfeld, 2004), and the ideas on control of information and personalisation presented here were developed solely by the author of the dissertation.

A further user study examining the invisibility problem (see section 2.3.5) and users’ perceptions of privacy and information sharing within intelligent environments was carried out using the MyPlace Visualisation Interface (MVI) (Carmichael, Kay & Kummerfeld, 2005) developed at the University of Sydney. The user study, described in section 4.5, was developed and conducted by the author of this thesis, and was originally published in the Australasian Computer-Human Interaction (OzCHI) 2005 conference (Chatfield, Carmichael, Hexel, Kay and Kummerfeld, 2005). The dissertation’s author was not involved in the development of the MyPlace architecture, so this work is included as background literature (see section 2.3.2.4).

Further research by the author and Dr Häkkilä (Häkkilä & Chatfield, 2006) into the users’ interaction with mobile device was carried out equally by both researchers. This research was published in the Nordic Conference on Human-Computer Interaction (NordiCHI 2006). However, as this research was not primarily directed by the dissertation’s author, it does not appear as a substantive part of this research. This study will be cited as per usual citation behaviour where appropriate (and is mentioned in section 2.5.2.4).

All other listed research publications were developed by the dissertation’s author, with guidance from my primary supervisor, Dr René Hexel.

1.5 Dissertation Outline

The dissertation is structured in the following way. Chapter two describes the background literature and research design prerequisites that are required to understand the research context and design. This chapter describes the relevant background literature on privacy and security within ubiquitous computing, and examines the structure of similar research and relevant methodological assumptions that influence our research’s design.

Chapter three examines the research questions addressed in the dissertation and builds on the previous chapter to describe the research path taken to address these research questions. This chapter considers the impact of the research activities undertaken and highlights a framework that allows the evaluation of our results in the context of other research. This chapter
describes all research activities carried out and provides easy reference tables and figures for the reader to refer to when considering how each research activity contributes to the greater research goals.

Chapter four describes the user tests carried out to develop our understanding of privacy and users’ privacy requirements within intelligent environments. These user tests examine users’ perceptions of information sharing, investigate the role of personalisation in ubiquitous computing environments, evaluate an initial privacy-aware architecture, and consider the role of ubiquitous computing in the development of digital communities and improving community connectedness.

Chapter five describes the research difficulties involved in developing a scalable intelligent environment architecture that can be integrated into users’ everyday lives. It discusses the identified problems in maintaining user privacy and security and the infrastructure required to support user interactions with intelligent environments.

Chapter six describes the Scalable, Privacy Aware Communication Environment (SPACE) architecture developed by the author as a solution to the lack of privacy and security within ubiquitous computing environments. This architecture allows interaction with ubiquitous computing environments without jeopardising users’ privacy or the security of their information. This architecture describes the control of information necessary to maintain user privacy within an intelligent environment, and examines the external entities required to manage user identity and to provide information security whilst utilising an intelligent environment’s services. A technical implementation of the architecture is evaluated.

Chapter seven discusses the SPACE architecture and examines how this could be used to integrate ubiquitous computing into our everyday lives. This analysis includes an examination of the dissertation's research questions and contributions. Chapter seven also considers the SPACE architecture's potential as a pervasive, ubiquitous computing infrastructure, its ability to improve community interaction and connectedness, and the role of user education in improving the privacy and information security outcomes of using the SPACE architecture.

The conclusions in chapter eight summarise the contribution of the dissertation to the current state of research and critically assess the limitations of this research. New areas of research that could expand the SPACE architecture are also identified. These include research into extending the 'disappearing computing' development ethos, improving the implementation and social integration of the SPACE architecture and extending the architecture using intelligent agents. The dissertation concludes with a statement on the outlook for ubiquitous computing and intelligent environments like the SPACE architecture.
Chapter Two: Background Literature

2.1 Introduction

This research examines the use of ubiquitous computing technologies to provide users with interactive intelligent services. More specifically, it examines intelligent environments, which are highly embedded, interactive spaces that seek to bring computation into real-world physical spaces (Coen, 1998). Ubiquitous computing is a term coined by Mark Weiser of Xerox Parc in 1988 (Weiser, 1991). Ubiquitous computing describes a new form of interaction with computing devices embedded in everyday objects. Weiser aspired that this new form of computing interaction would be a method of reducing the cognitive load of computing devices on users, as users focus on the task at hand and not on the computer itself. This effectively pushes computers into the periphery of human consciousness and to the background of any given user interaction.

This chapter examines how ubiquitous computing could potentially be used in our everyday environments\(^1\). It begins by looking at how ubiquitous and distributed computing systems are used in our current world, and the concerns users of these environments might have. It then examines the nature of privacy and any privacy concerns that users may have with the use of these systems. Security in distributed environments is then examined to determine its effectiveness in providing users with privacy through information security.

The described background literature has influenced the development of many intelligent environments. These intelligent environments are further studied to understand what user privacy and information security their architecture provides. The analysis considers the design strategies used to minimise risks to user privacy and the technical details of securely exchanging information using ubiquitous computing technologies.

2.2 The Digital Society

The effect of the Internet and similar advances in communication technologies has led many to consider the direction in which our society is heading. News reports and political rhetoric talk about the shrinking world, the interconnectivity of markets and necessary global solutions to problems that affect all of us. Internet search engines and online news media make information available from all over the world, exposing users to new cultures, religions and opinions. But what effect is this having on the people who use these technologies? How could new technologies, like wireless network access

---

\(^1\) In the dissertation, 'Everyday Environments' means the physical environments that users might normally enter in their daily life (for example a user’s home, office, transportation networks, street malls, shopping centres, bars, coffee shops and museums).
or improved device functionality and miniaturisation, be used to improve their lives?

An initial look into emerging digital culture was carried out soon after the Internet was becoming widely available. The Digital Citizen survey (Katz, 1997) was carried out to investigate the motivations, characteristics and activities of people either using or not using the Internet and various communication technologies. The results of this survey separated respondents into groups based upon their interaction with the Internet, and identified the views of each group on many social, political and economic issues. These groups can be broadly classified as ‘Connected’, including ‘Connected’ and ‘Superconnected’ users, and the ‘Unconnected’ (Katz, 1997).

Those in the overall ‘Connected’ group are the ‘Digital Citizens’ that make use of the Internet and communication tools to remain more in touch with their world. These Digital Citizens are for the most part knowledgeable, tolerant, civic-minded, political, well-educated and radically committed to change (Katz, 1997). This group is also profoundly optimistic about the future, they are convinced that technology is a force for good and that free-market economies are powerful engines of progress. This group is not about new gadgets, being trendy or cultural domination. They are more about giving individuals a taste of democracy, helping them create new kinds of communities and reconnecting them with the institutions that shape their daily lives. It is about sharing knowledge and information, and spreading ideas and prosperity (Katz, 1997).

This exploratory look into the new world, however, is dated. A majority of modern computer users would fall into the ‘Superconnected’ group, having access to a laptop, home computer and mobile phone and using email more than three times a week. Phones are bringing email and text communication to a wide audience. The uptake of mobile phones, messenger programs, email and the Internet amongst young people is changing the way the next generation is accessing and sharing information. Katz (1997) concludes that the digital citizen’s sense of ‘community’ is much more important than the hardware or technologies used. The dissertation’s research seeks to present new interaction opportunities that could improve the connection these users have to their community and the environments in which they live.

The influence the Internet is having upon our daily lives is aptly demonstrated by the proliferation of users using online blogs, reaffirming the ‘digital citizens’ proactive engagement in issues they’re passionate about, and by the rise of citizen journalists commenting on news and sharing newsworthy footage captured on mobile phones and digital cameras. This new-found ability to reach large numbers of people cheaply, for example by using blogs or message boards, has allowed Internet users to harness great social pressure against previously unassailable opponents like governments or multinational corporations (Zureik & Mowshowitz, 2005).

Not all moves towards greater digital connectivity are positive, especially when we consider the impacts of these technologies on our communities. With the increasing use of computer-mediated communication (CMC), we are
moving from our sense of community as a neighbourhood to a sense of a community as a social network (Wellman, 2005). The increased saturation of mobile communication technologies and the design of modern suburban cities are disconnecting people from their community (Oldenburg, 1999). This reduces the benefits that people derive from their casual interactions with their local community.

The same technologies, however, also provide opportunities for new types of communities to develop. In today's world a community is comprised of a dynamic collection of friends, relatives and work colleagues that interact irrespective of physical locality. This computerisation of communication adds a layer of richness to our interactions, filling in the time between face-to-face contact and providing new interaction opportunities. The ease and speed at which new software and social networking tools (e.g. Facebook or MySpace) spread across the globe via the Internet allows the rapid evolution of social networking tools and provides new ways for users to interact when not co-located.

As we increasingly integrate these technologies into our lives, there comes a point where we all become ‘Digital Citizens’ to some degree. Broadband Internet access is becoming omnipresent, the mobile phone market is approaching saturation point world-wide and email is rapidly becoming the preferred communication medium for those outside our circle of close friends and family. The availability of these technologies provides many new opportunities for information service delivery and the convergence of new features onto existing hardware, for example, the addition of Internet browsers, cameras, music players and torches into mobile phones. There is a need to examine how these new technologies may be integrated into users’ worlds. New access to information services and digital communities must be tempered by their relevance to users, and their ability to deliver these structures without risks to users’ privacy and information security.

### 2.2.1 Distributed and Mobile Computing

A distributed system is one in which components located at networked computers communicate and coordinate their actions only by passing messages (Coulouris, Dollimore & Kindberg, 2001). These systems have changed the way we can interact with each other, allowing new services and indeed new communities to be developed. In twenty-five years the Internet has changed from a collection of networked research computers into the lifeblood of the world’s news, communication, entertainment and commerce.

In the last ten years the availability of mobile computing has exploded, especially with the advent of wireless communication technologies like WiFi or Bluetooth. Mobile phone ownership is reaching saturation point in many markets, with the number of mobile phone subscriptions surpassing 2 billion in 2005 (Lee, 2005). Digital communities across the Internet are providing new forums for likeminded people to interact, playing online games and trading goods and services. In the continued development of the digital society, we must consider what distributed systems could provide useful new
forms of interaction while allowing users to maintain their desired level of security and privacy.

The sheer pervasiveness of mobile phones and handheld computers brings opportunities for people to interact with the new digital community from everyday environments. However, there are many challenges facing the development and adoption of distributed computing systems. The challenges that arise from the construction of these systems are the heterogeneity of components, openness, which allows components to be added or replaced, security, scalability, failure handling, concurrency of components and transparency (Coulouris, Dollimore & Kindberg, 2001). Security and scalability have particular relevance to ubiquitous computing systems, and they could potentially be made up of thousands of simple, physically accessibly components.

The communication of messages between components can also produce unexpected privacy problems for users. Mobile phones, for example, can be located by triangulating their signal strength between multiple signal towers (Hightower & Borriello, 2001). Users walking in and out of multiple ubiquitous computing environments can be tracked, and patterns of movements can be inferred and used to predict their current location (Beresford & Stajano, 2003). The security of wireless information transfers, particularly between relatively simple devices, can easily be compromised.

Usable and useful ubiquitous computing systems must be relatively open, highly scalable and attractive to users. They must therefore provide useful services in a private and secure manner. However, the very nature of many ubiquitous computing systems puts them at odds with these goals. The collection and storage of information about the environment, and the users within it, can breach users’ privacy. The openness and location of system hardware within the environment can make it difficult to secure.

2.2.2 Ubiquitous Computing

The natural emergence of technology frequently brings times when society must adjust to, and seek to understand, the role that this technology could have in our everyday lives. Ubiquitous computing is currently in the same position where the Internet was in the 1980s: the technology for accessing computers across TCP/IP networks was understood, but the development of web pages and e-services was unheard of. Ubiquitous computing literally means ‘computers everywhere’, and the term has been adopted to mean the embedding of computers into our current environments to provide context-aware services.

Marc Weiser saw that, rather than being ‘a tool through which we work, and thus disappearing from our awareness, the computer too often remains the focus of attention’ (Weiser, 1993). This suggests that, not only are we seeking to integrate our computers into our everyday environments, but these environments must overcome the current problems of using traditional computers and make their use easier. Simply put, ubiquitous computing devices should not create alien work environments, but they should be used
to improve our interaction within our current environments. Computers should make up an invisible foundation that is quickly forgotten but is always with us, and is used effortlessly throughout our lives (Weiser, 1994). This integration into our everyday lives is the focus of this research.

Ubiquitous computing therefore describes a paradigm shift away from the idea of computers as discrete systems that users interact with for a particular purpose (e.g. gaming or word processing), towards the idea of integrated computer networks covering out everyday lives. Ubiquitous computing environments use embedded sensors and processors to gather and organise information in order to assist with other tasks or services. The development of ubiquitous computing environment (and the required infrastructure) for an organised purpose (e.g. personalised service delivery) in a particular physical environment is known as an intelligent environment (see section 2.3).

2.2.2.1 Ubiquitous Computing Technologies

Ubiquitous computing describes technology that is embedded into its environment in a manner that makes it all but invisible. Ubiquitous computing environments can make use of sensors distributed throughout the environment, micro-chips embedded in clothing and everyday items, small handheld computers and a huge variety of input tools (e.g. smart pens or pointers). While this implies the use of simple embedded processors, these are normally deployed in a network with more advanced processors and mobile computing devices. The advanced processors correlate information and provide services, while the mobile devices provide user interaction with services and can manage information exchanges with the ubiquitous computing environment. While the ability to collect information behind the scenes can provide users (or the environment’s owners) with useful services (or other benefits) there are many risks associated with their use.

Problems with these computing devices vary with their type, but include a lack of computational power (for encryption), physical insecurity (they can be physically hacked or broken), limited battery power and lack of user input and display devices for interaction with these devices (Stajano, 2002). Furthermore, their use within existing user environments can be ineffective or controversial. For example, the use of sensors to capture information from an environment must wrestle with issues of user privacy, while the storage of information on hardware susceptible to physical tampering can cause significant security risks.

The emergence of wide-area networks and cheap computer chips has revolutionised how we think about access to computers. Wireless networks have evolved from a building- and campus-wide scale to be implemented across entire cities (Associated Press, 2006) and in some cases entire countries (Reid, 2005). The price of radio-frequency identity tags (RFID-Tags) have dropped to a point where it is now cost effective to embed them on each product for inventory tracking, and near ubiquitous handheld mobile phones and PDAs have provided ideal platforms for user interaction wherever they go. Research into this area must ask the question: how can we leverage
these new technologies to provide safe and useful services for users in their current environments?

2.2.2.2 Ubiquitous Computing Environments

Ubiquitous computing technologies have already been incorporated into real-world environments for gaming and entertainment purposes. Mixed-reality games use a combination of players in the real world and online to provide a unique gaming experience. These games developed from access to cheap communication tools and global positioning systems, and are the latest evolution of augmented reality (e.g. arQuake (Thomas, Close, Donoghue, Squires, De Bondi and Piekarski, 2002)), location-based gaming and recreation activities (e.g. Human Pacman (Cheok, Goh, Liu, Farbiz, Fong, Teo, Li and Yang, 2004) and Geo-caching (http://www.geocaching.com/)). These activities provide us with an opportunity to examine users' interactions within ubiquitous computing technologies.

An important aspect of the mixed-reality games was the developing of strategies to effectively engage in the game and environments. This is evident in the coordination between players of the ‘Can You See Me Now?’ game run in Nottingham and Sheffield (Anastasi, Tandavanitj, Flintham, Crabtree, Adams, Row-Farr, Iddon, Benford, Hemmings, Izadi and Taylor, 2002), where players moving around on an online map attempted to outrun players (the ‘runners’) being tracked via GPS in the real world. Players used text messages to educate new users about the environment and to coordinate strategies for successfully playing the game.

The use of identity in the game is interesting, as players used recognisable, repeatable pseudonyms when communicating, but the interactive map provided no visual clues to identity. This was overcome using text messages to clarify a user’s position and to coordinate strategies to achieve a common goal. This common goal is missing from service-orientated ubiquitous computing environments, which reduces the need for social coordination with other users within the environment. This will not always be the case, and it is likely that alternative reasons for wanting to communicate with local users (beyond casual social interaction) will develop (e.g. sharing information on public transport delays, etc.). The use of ubiquitous computing technologies to deliver computing and information services within real-world environments is discussed in section 2.3.

2.2.3 Digital Communities

The digital society is so named because of the increasing amount of time people spend interacting with the Internet (and computers) for work and leisure. People are increasingly interacting on the Internet with specific communities that share their personal interests. These communities are loosely organised to support entertainment preferences (e.g. movies and books), hobbies, online games, social networking, news and political commentary and many others. They may further be differentiated geographically or through various variations on the above themes (e.g. local or country-specific news).
Second Life (http://www.secondlife.com/) is a virtual world that allows users to create their own landscapes, interact with other users and recreate most real-world activities. Sites like MySpace (http://www.myspace.com/) and YouTube (http://www.youtube.com/) provide user interaction forums nominally based around the sharing of multimedia content. Slashdot (http://www.slashdot.org/), Digg (http://www.digg.com/) and Reddit (http://www.reddit.com/) are popular news aggregation sites that encourage discussion between users. These online communities are valuable as they allow users to interact with like-minded, geographically dispersed people. They do not, however, support the local community where the users live.

The P3 Framework (Jones, Grandhi, Terveen and Whittaker, 2004) examines context-aware community and user-based interaction systems that are either people- or location-centric. These systems support personal interaction such as opportunistic communication with colleagues and friends, social matching and the maintenance of social networks. Place-centred services include social navigation, task coordination and communication about places and activities. The ActiveCampus project (Griswold, Shanahan, Brown, Boyer, Ratto, Shapiro and Truong, 2004) is a ubiquitous computing environment with community interaction, directions and local information services. The ActiveCampus project demonstrated the benefits of improving community interaction inside classrooms, but privacy issues remained and casual community interaction was limited, with users overwhelmingly (91.5%) rejecting the exchange of location and presence information with other (non-buddy) users.

In his book *The Great Good Place*, Ray Oldenburg describes the impact of ‘third places’, for example, coffee shops, libraries, clubs etc., where community members meet and interact. Third places promote casual social interactions between community members and are ‘at the heart of a community’s social vitality and the grassroots of democracy’ (Oldenburg, 1999). Oldenburg described the phenomenon of communities losing their third places to the suburbanisation of our cities, which limits access to third places, and to the increasing cost of entertainment or ‘going out’, which alters a third place’s nature, accessibility and social value. This loss erodes the social, economic and personal benefits people derive from casual interactions with their community.

As our societies lose places for ‘casual interaction’ amongst the people, there is a trend towards individualism and disengagement from the greater community. The traditional sense of ‘community’ is being replaced by personally centralised groups of friends and family that maintain their own sense of community. These collectives, variously described as social networks or urban tribes (Watters, 2003), provide the support and casual interactions ‘missing’ from modern urban environments. Wellman describes this change from place-to-place to person-to-person communication as Networked Individualism (Wellman, 2002), as micro-communication with our ‘tribe’ replaces casual social interaction with our community.

These urban tribes, via new communication methods and evolving social practices, are supplementing or replacing the socialisation that once took place in ‘third places’. Through friend-of-friend associations and the
overlapping of different social groups, people are exposed to a wide range of people, which is similar to community gatherings in a public space. This new phenomenon could be called a symptom of the modern community, or of modern communication tools (i.e. it is now possible to maintain contact with a select group of friends (or a particular sub-community) and to spurn all contact with the local community). Any solution to improve local community interaction should address not only the lack of third places in our communities, but should also leverage the interactions and relationships within our urban tribes.

Oldenburg believes that America has a ‘problem of place’ because ‘the automobile suburb has the effect of fragmenting the individual’s world’ (Oldenburg, 1999, p. 4), and the benefits third places have upon a community are slowly being eroded by compartmentalised town planning and changes in consumer’s lifestyles and community interaction. The extent to which this continues today is arguable, but this research does raise interesting questions as to how we might support local community interaction. The nature of third places makes them difficult to replicate or support using technological means.

To consider how we might provide this support, it is useful to consider the specific characteristics of Oldenburg’s third places:

- they are on neutral ground;
- they are a social leveller;
- conversation is the main activity;
- they are accessible;
- they act as a home away from home and have ‘regulars’; and
- the mood is playful.

Attempts have been made to recreate third places using computer-mediated communication (CMC) environments like chatrooms, multi-user environments or bulletin board systems (e.g. (Kendall, 2002; Schuler, 1996)). Soukup (2006) provides us with a systematic evaluation of the extent to which CMC systems (or ‘virtual communities’) fulfil the roles of the third place. Virtual communities do provide a neutral third place away from the demands of work and home life (Kendall, 2002) where regulars can meet for ‘playful and fun’ conversations or interactions (Schuler, 1996). This playfulness is often promoted by the types of interactivity and identity concealment (or use of a persona) common in virtual communities (Danet, 2001). But Soukop (2006) identifies three problems with these computer-mediated environments: they do not emphasise a localized community, they do not provide a social levelling place of interaction, and they are not accessible.

Oldenburg asserts the importance of geographically situated community interaction in his second edition preface: ‘The first and most important function of third places is that of uniting a neighbourhood’ (Oldenburg, 1999, p. xvii). But computer-mediated environments are rarely used by members of the same physical community; indeed they ‘are unique because they transcend physical space, offering communication opportunities outside their community’ (Schuler, 1996). Any ‘virtual third place’ must therefore be either physically collocated in the local community, or should be primarily used by
members of the community while discussing issues relevant to that community. Virtual communities tend to have specific target audiences based upon a common set of interests or beliefs (e.g. entertainment, sporting, religious or political topics), while third places suggest a commonality based upon where people live. The latter leads to an informal meeting place where social positions tend to be less important, while the former leads to a knowledge-based social hierarchy counterproductive to relaxed social engagement and community integration (Schuler, 1996).

Accessibility of the third place by all is also essential for greater community involvement and integration. Access to ‘virtual communities’ is, by definition, limited to those with access to the Internet. This creates barriers of access and prevents the engagement of the entire community. But technological access alone is insufficient to solve accessibility problems. Virtual communities are much more effective when coupled with well-designed (and culturally aware) training (Keeble, 2003), and social connection and informal interaction are essential to promoting community interaction and participation (Liff & Steward, 2001). Third places should also be constructed by (or in consultation with) participating members of the community.

Soukup (2006) identifies ‘presence’ as a final requirement of ‘virtual third places’ in constructing a welcoming home away from home. Presence describes the ‘sense of being in an environment’ (Steuer, 1995) or the degree to which the virtual third place promotes users to feel immersed in the environment (Soukup, 2006). This sense of immersion is integral to users’ acceptance and ownership of the space, and will determine the extent to which the community becomes engaged in the environment. Environments should look and feel (as much as possible) like the communities they represent, and creative use of animation, three-dimensionality and characterisation of identity (e.g. Avatars or personae) should be used to enhance the process of localisation and presence (Soukup, 2006). These guidelines highlight the importance of connecting the user to the community, and not of the delivery of a complete multimedia experience.

Acknowledging the importance of third places leads us to consider if we could use ubiquitous computing technologies to support and promote digital communities that can effectively act as ‘third places’. Whilst there is limited evidence for the effectiveness of third places in creating community connectedness, this does provide a useful starting point when considering how to develop interaction and persistent community engagement spaces. This research considers how our proposed ubiquitous computing infrastructure could incorporate not only these digital communities, but how it could also incorporate the communication tools necessary to coordinate with the user’s ‘Urban Tribe’. The place of digital communities within our ubiquitous computing infrastructure is described in section 5.2.1.

2.2.4 Summary and Conclusions

The emergence of the Internet over the last twenty years has led us to the current tipping point. It is not only possible to deliver users personalised, contextualised ubiquitous services, but there is now a huge potential audience
that could easily integrate the use of ubiquitous computing services into their everyday lives. These environments have begun to be developed, but they are currently being developed in isolation and mostly without thought to the social problems associated with their use. This research seeks to develop a complete ubiquitous computing infrastructure that can provide context-aware services and community interaction forums.

Digital communities are community-accessible interaction forums that try to replicate the social connectedness found in more traditional third places. It is hoped that these interaction spaces will help support local community interaction and be of some value to their community. Digital communities have, however, failed in the past to provide these benefits. In particular they have failed to provide a socially unrestricted interaction space, failed to emphasise the local community and failed to be accessible to the entire community. These failures are as much social, political and economical as they are technical (perhaps even more so), but they must be addressed if we are to successfully provide digital third places through our ubiquitous computing infrastructure.

The ‘Intelligent Environments’ described in the next section demonstrate the current state of the art of the development of these ubiquitous computing environments. These examples give us an excellent understanding of the ability of the current wireless networks and personal mobile devices to deliver contextually-aware services. The section also highlights particular concerns of using intelligent environments, including context awareness, personalisation of service delivery and the representation of knowledge. This research forms the basis for understanding how our digital communities can be integrated into our everyday lives using the proposed ubiquitous computing infrastructure.

2.3 Intelligent Environments

Coen (1998) defines intelligent environments as highly embedded, interactive spaces that seek to bring computation and digital services into real-world physical spaces. Ubiquitous computing devices are used to collect and correlate information in the environment, and this information is used to provide services to the environment’s users or owners. Services could be provided directly to the user (e.g. on a public display) or more usually to their mobile device. Intelligent environments differ from basic ubiquitous computing environments due to the complexity of the interactions available, and the infrastructure required to support this interaction (e.g. the service providers and identity management structures).

An intelligent environment architecture describes the components of the system embedded in the environment, their inter-relationships and any communication with users (or their mobile devices) and other external systems. Intelligent environments could potentially only provide information to the environment’s owners, but this collection of information beyond the awareness of users represents poor ubiquitous computing design and is a significant privacy concern for users. This type of surveillance and information
collection, and its impact on user’s privacy, is discussed throughout section 2.4.

This dissertation’s research is particularly inspired by Mark Weiser’s work on ubiquitous computing, and by the desire to move beyond the current computing interaction paradigm to allow more effective use of computing technology (Weiser, 1991). Intelligent environments take advantage of technological developments in hardware miniaturisation, multimodal human-computer interfaces and wireless communication devices and protocols to develop new forms of computer interaction. These advances allow physical environments to be embedded with information and environmental services that can react to observed and predicted user needs. The use of intelligent environments is illustrated by the following scenario.

Belinda works in a hospital a short bus ride from her house and she takes the bus to work each day. She carries a smart phone that allows her to interact with the intelligent environments in her home, on the bus and at work. When Belinda boards the bus in the morning, her smart phone provides the environment with her yearly bus pass number, properly authenticated by the bus company, and she and the driver hear a soft beep acknowledging the validity of her pass. During the journey, a nearby monitor recognises she is the only person nearby and switches to her favourite channel. When she arrives at the hospital, her daily schedule downloads itself to her phone, including the condition of her patients, and she walks to the staff lounge to change her coat. The lounge door senses when she is close and opens the door for her.

This scenario describes a few simple examples in which an intelligent environment reacts to its immediate context and provides a service that does not require explicit input from the user. The implied collection, storage and use of information carries with it complex problems of privacy and security that have to be answered before these systems will be acceptable for mass implementation within our world, but the benefits of developing them make these problems worth solving. This research seeks to develop a privacy and security-aware intelligent environment architecture.

The P3 Framework (Jones et al., 2004) considers the types of systems supported by intelligent environments, highlighting the current focus on people-to-people and people-to-geographical places interaction. These people-to-people systems support personal interaction such as opportunistic communication with colleagues and friends, social matching and the maintenance of social networks. Place-centred services include social navigation, task coordination and communication about places and activities. Intelligent environments will cover all aspects of our lives, from our homes, workplaces and cars, to all manner of public spaces. This unprecedented coverage of our lives allows for extensive collection of information about our activities, habits and feelings (Lahlou, Langheinrich & Röcker, 2005).

Drawing on their work developing privacy design guidelines for disappearing computing environments (Lahlou & Jegou, 2003), described further in section 2.4.2.1, these authors identify the major problems with the information
sharing within smart or intelligent environments (Lahlou, Langheinrich & Röcker, 2005). These are as follows:

- unprecedented coverage of these networks across our everyday lives;
- the invisibility of the data collection activities;
- the intimate and extensive nature of the data collected and inferred about our activities, habits and feelings;
- the underlying motivation for this data collection to allow the environments to anticipate our actions and desires; and
- the increasing connectivity of these environments, and the impact this has on the environments’ ability to infer much more about users, and effectively allowing no privacy whilst within their coverage.

Lahlou et al. (2005) warn of the dangers of such unprecedented collection of users’ personal information and the lack of awareness of the privacy concerns amongst developers in this area. This lack of awareness often manifests itself in the lack of privacy guidelines at a design level, and this prevents privacy considerations being implemented when they have any chance of success (at the design level). Users’ unwillingness to trust ubiquitous computing systems is seen as the major impediment to acceptance of these systems (Langheinrich, 2001).

Intelligent environments seek to support a user’s interactions within their existing environments. Designers must therefore support users’ social behaviour and recognise the social implications of pervasive technology, as much as providing users with new ubiquitous computing services. The social implications of using intelligent environments include dangers to user privacy and information security, difficulties ensuring system visibility to users, and difficulties in providing users with effective control over information sensing activities (Abowd, GD & Mynatt, 2000). The dissertation must therefore identify a way of addressing these privacy and security concerns at the design level to ensure user acceptance and use of ubiquitous computing environments.

Present research into ubiquitous computing concentrates predominantly on separated insular environments. The research examines everything from the development of new pervasive computing components to the integration of sophisticated context management systems into real-world environments. This initial development is an important part in the maturation of any new technology, but there still remains a scarcity of systems, considering the scalable, ubiquitous and interoperable nature of these systems. It is now important to consider the place for intelligent environments in our world, and to develop a generic framework for their integration.

2.3.1 Intelligent Environment Examples

This section describes existing intelligent environments and pervasive computing research projects. These systems and projects allow us to consider the nature of the developed systems, and to get a sense of the current state of the art in the development of ubiquitous computing environments. Where appropriate, intelligent environments listed here are described further in section 2.3.2.
MIT’s project Oxygen is a human-centric pervasive computing effort that combines research and industrial involvement (MIT, 2004). This project was developed following the premise that, in the future, computation will be human-centric and freely available, much like oxygen in the air we breathe, and will allow users to make use of this computation to support everyday tasks. The project rests on an infrastructure of mobile and stationary devices connected by a self-configuring infrastructure (Coen, Phillips, Warshawsky, Weisman, Peters and Finin, 1999). A number of pervasive computing systems have been developed under this project umbrella, including Activity Zones (Koile, Tollmar, Demirdjian, Shrobe and Darrell, 2003), Metaglue (Coen et al., 1999) and the cricket systems (Priyantha, Chakraborthy & Balakrishnan, 2000).

Microsoft’s EasyLiving project investigates the technologies required for an intelligent environment prototype. EasyLiving concentrated on applications where interactions with computing can be extended beyond the normal desktop model (Brumitt, Krumm, Meyers and Shafer, 2000). This project developed as a test-bed for many ubiquitous computing concepts and designs, and developed a vision-based Person Tracker (Brumitt et al., 2000) in order to construct a geometric model of the environment and its context. Long-term challenges identified by the EasyLiving project include the need for intelligent environments to be Secure, Private, Accessible, Extendable and to manage the complexity of these environments.

Iachello, Smith, Consolvo, Abowd, Hughes, Howard, Potter, Scott, Sohn, Hightower and LaMarca (2005) investigated information sharing using a peer-to-peer, mobile, location-enhanced messaging service. This study investigated the value of simple location-enhanced messaging and examined current ‘Find-a-Friend’ services. The 11 participants in the extended user study rejected the need for automated messages with location information, instead preferring the plausible deniability of user-initiated messages. These messages can provide users with the desired privacy without requiring the user to give false information, and can facilitate complex social negotiations not possible with automated location-based information sharing.

The three design suggestions recommended by this study are: do not make automated functions a design priority, lightweight messaging systems have great potential to simplify and support awareness and mobile messaging systems, and ubiquitous computing systems should explicitly support plausible deniability (Iachello et al., 2005). This calls for a user-centric view of information sharing and control of interactions within ubiquitous computing environments. This supports users in selectively enhancing their interactions with the real world, without endangering their privacy. The study’s evaluations of existing location-based ‘find-a-friend’ services found that proprietary messaging formats locking out users of other system restricted their accessibility and lowered their value (Iachello et al., 2005). Intelligent environments must allow plausible deniability, provide easy to use, non-automated functionality, and use non-proprietary networks or technologies.

The Personal Server is ‘a mobile system designed to enable interaction with a user’s personal data through the surrounding computing infrastructure’
(Want, Pering, Danneels, Kumar, Sundar and Light, 2002). The personal server contains no user displays, but instead it co-opts the screens and keyboards of nearby computers through a short-range wireless link. In addition to short-range communication, the personal server contains enough high-density storage and low-power, high-performance processing to serve a user’s mobile computing and storage needs (Want et al., 2002). This allows users access to their own information and applications that are stored on the server, without relying on the limited interface and displays common on small handheld devices.

The Portolano project (http://portolano.cs.washington.edu/The Portolano Project) at the University of Washington seeks to create a test bed for investigation into the emerging field of invisible computing. The devices developed in this project are so highly optimised to particular tasks that they blend into the world and require little technical knowledge on the part of their users. This project has had several significant outcomes. Labscape is a pervasive computing system for monitoring activities in a science laboratory (Arnstein, Borriello, Consolvo, Hung and Su, 2002). The Location Stack project has developed methods for sensor fusion for context-aware systems (Graumann, Lara, Hightower and Borriello, 2003). The Portolano project proposes an infrastructure based upon mobile agents that interact with environmental applications and users (Saha & Mukherjee, 2003). Data-centric routing automatically migrates data amongst the user’s applications on their behalf. Data thus becomes ‘smart’, and serves as an interaction mechanism within the environment.

Georgia Tech’s Aware Home project (Kidd, Orr, Abowd, Atkeson, Essa, MacIntyre, Mynatt, Starner and Newstetter, 1999) has developed a large number of pervasive computing systems and applications aimed at supporting users’ computing needs in their everyday world. This project focuses on pervasive computing environments in the home, and has developed a number of methods to track users via ultrasonic sensors, RF technology and video recognition through floor sensors and vision techniques (Kidd et al., 1999). This project was developed from the Classroom 2000 project, which was a pervasive computing environment that instrumented a classroom environment to enable the recording of live lectures (Abowd, 1999). An important contribution of this research, identified through the everyday use of ubiquitous computing environments, is the need to give the occupants knowledge and control of the distribution of any information collected in such a heavily monitored environment (Kidd et al., 1999).

The Equator project (http://www.equator.ac.uk) is a six-year Interdisciplinary Research Collaboration (IRC) effort supported by the Engineering and Physical Sciences Research Council (EPSRC) that focuses on the integration of physical and digital interaction. The name symbolised an ideal: the ability to cross the border between physical and digital experience without a thought, thereby enabling each environment to complement the other, as equals in a kind of dynamic balance. Since 2001, the Equator project has published hundreds of research papers and technical reports, and has examined new methods of computer interaction (Gaver, Bowers, Boucher, Gellerson, Pennington,
Schmidt, Steed, Villars and Walker, 2004), the interaction between virtual and physical spaces (Dix, Friday, Koleva, Rodden, Muller, Randell and Steed, 2005), and the creation of games (Flintham, Anastasi, Benford, Hemmings, Crabtree, Greenhalgh, Rodden, Tandavanitj, Adams and Row-Farr, 2003) and learning platforms (Price, Rogers, Stanton and Smith, 2003) that integrate the virtual and real worlds. The Equator project has evolved to begin questioning its own underlying assumption: do users always want a seamless divide? This question should be incorporated into any study of how best to deliver ubiquitous computing environments and services to users.

The HIT Lab (New Zealand) is a Christchurch based laboratory that focuses on the overlapping areas of computer-supported cooperative work, tangible user interfaces and perceptual user interfaces. Many of the current projects are focused on the use of Augmented Reality systems for human-computer interaction (http://www.hitlabnz.org/). The Enterprise Distributed Systems Technology Centre (eDSTC) is a Queensland-based cooperative research centre (CRC) that has research projects, technologies and spin-offs relating to pervasive computing. The most well know is Elvin (Segall, Bill & Arnold, 1997), the publish-subscribe system that is used around the world for deploying loosely coupled component-based systems that typify ubiquitous computing environments.

The Smart Internet Technology CRC (http://www.smartinternet.com.au/) is a collaboration of Australian researchers and commercial partners that, amongst other activities, examines pervasive computing, and more specifically Intelligent Environments and Natural Adaptive User Interfaces common in ubiquitous computing. Of particular interest from this group is the Merino (Kummerfeld, Quigley, Johnson and Hexel, 2003) and MICA (Kadous & Sammut, 2004) projects that develop potential architectures for ubiquitous computing networks, and Nightingale (Risborg & Quigley, 2003), which investigates users’ interaction with ubiquitous computing delivered services.

The Merino project developed an Intelligent Environment architecture (Kummerfeld et al., 2003) that uses information abstraction to maintain users’ privacy and to manage information within the intelligent environment. The Multimodal Inter-agent Communication Architecture (MICA) project constitutes a middleware system for multi-model application support in pervasive computing (Kadous & Sammut, 2004). The Nightingale project constitutes a data, context and application architecture for Pervasive Computing (Risborg & Quigley, 2003). This system supports a personal and peripheral area network to provide invisible or natural interfaces for reminiscence applications for the elderly.

### 2.3.2 Intelligent Environment Architectures

Ubiquitous computing environments have progressed from the initial generic identification of its purpose, set out by Weiser (1991), to a more formal understanding of intelligent environments and their purpose (e.g. Coen, 1998). Intelligent environments have since been developed to test user interaction methods (Coen et al., 1999), provide feedback on security (Campbell, Al-Muhtadi, Naldurg, Sampemane and Mickunas, 2002) or users’
privacy issues (Lahlou, 2005) and provide pervasive computing middleware to support ubiquitous computing services (Cutting, Hudson & Quigley, 2004; Saha & Mukherjee, 2003). More recent research has developed architectures that model users’ and environmental information (Carmichael, Kay & Kummerfeld, 2005; Kummerfeld et al., 2003) and provide methods of accessing ubiquitous computing services whilst considering the impacts of this access to users’ privacy and information security (Modahl, Agarwalla, Saponas, Abowd and Ramachandran, 2006). This section examines different intelligent environment architectures and highlights interesting features that will be incorporated into the architecture developed in this dissertation.

2.3.2.1 Merino Scalable Intelligent Environment Architecture

The Merino architecture facilitates scalable information sharing between users and intelligent environments (Kummerfeld et al., 2003). In particular, the architecture allows the sharing of contextual information about the current physical and computational environment. This information is shared at increasingly more abstract levels to ensure the integrity of users’ privacy (Kummerfeld et al., 2003). This architecture provides a framework for the management of environmental context data that enables sophisticated pervasive computing services in a scalable manner.

The proposed architecture for the intelligent environment is central to determining methods for capturing information at the sensor level, interpreting by historical reference, and aggregating into increasingly more abstract forms (Kummerfeld et al., 2003). The Merino architecture, shown below as Figure 1, describes the layers of context that provide the basis for the abstraction of information. These layers are:

- Smart Sensors Layer
- Smart Environment Agents Layer
- Rich Context (represented as the IE Repository)
- User Model (the internal representation of the user and their interaction requirements)

![Figure 1: Merino Abstraction of an Intelligent Environment (Kummerfeld et al., 2003)](image-url)
The Smart Environment Agents use information from many sensors (or from Smart Sensors which correlate and process information from numerous sensors) to build the rich context for the intelligent environment. The User Model provides the intelligent environment with user information and interaction preferences that are used in conjunction with the IE Repository to provide tailored services to the user. Access to information is governed by the layer of abstraction at which it is found. For example, access may be granted to any user to determine whether someone is in his or her office (the user in this case has access to information found in the Smart Sensors layer), but access to the working habits of another office user would generally be unavailable (the user would not have access to the Smart Environment Agents or IE Repository).

At each layer of this architecture there exists the need to incorporate measures to preserve user privacy. User feedback describing the flow of information within the environment should be as comprehensive as possible, but must not create a burden on the user. The Merino architecture supports the management of the two-way flow of information critical to the perceived and actual integrity of user privacy. But the Merino architecture is vague on user interaction (especially across multiple intelligent environments), does not explain how users can interact with the environment with different identities (or manage the collection of their personal information) and does not consider the potential for the intelligent environment to be untrustworthy. These shortcomings must be addressed in the architecture developed by the dissertation.

2.3.2.2 Framework for Intelligent Instrumented Environments

Stahl (2002) developed a framework for intelligent instrumented environments that also provides abstract layers for sensor input, knowledge representation and human-computer interaction. The author describes sample intelligent environments that provide a multitude of services. His representation framework describes the framework necessary to manage the information from these services, sensors and interaction with the user. Stahl’s representation of the intelligent environment (2002) is similar to the Merino architecture’s use of abstraction of information layers within the intelligent environment (Kummerfeld et al., 2003).

Stahl advocates implementing a ‘knowledge representation layer’ as a common language among the entities within the environment (2002). The intelligent environment requires a ‘sensor input layer’ to handle inputs into the environment from the ubiquitous computing sensors, and advocates the use of temporal, spatial and semantic scopes to constrain the flow of information within the environment. Finally, the framework identifies the need for a ‘human-computer interaction layer’ to interact with all forms of inputs and outputs from users within the environment.

Stahl’s framework suffers from similar problems to many of the intelligent environment architectures currently in development. Privacy in this environment is not addressed, nor is there any concept of how this system could be scaled to cover multiple environments. The small scope of the
doctoral paper does not allow for a description of how the temporal, spatial or semantic constraints on information are to be applied, or how the user’s information would be secured from the intelligent environment. Nor is it clear how users can use intelligent agents within this environment without having their agents’ goals or identity being accessible to the environment; this could be a major privacy concern as it could allow the collection of the user’s goals or tracking of their agents’, and therefore their own, movements throughout the intelligent environment.

Intelligent Agents have been suggested for use in other intelligent environments (Coen et al., 1999; Johanson, Fox & Winograd, 2002), but these intelligent environments are self-contained, and they make the assumption that all agents are trustworthy, non-mobile (outside of the system) and have free access to all resources (Kottahachchi & Laddaga, 2004). This is unlikely to be the case. Furthermore, intelligent agents require users to give up control of much of their interaction with an intelligent environment’s services, which this research identified early that users are reluctant to do at this stage of ubiquitous computing development (see results in section 4.2). While there is ultimately value to be had in using intelligent agents to manage or support users’ interactions with multiple intelligent environments, it is well outside the scope of this PhD research and therefore is discussed as future research in section 8.3.4.

The architectural components described by Stahl (2002) are similar to the Smart Sensors, Smart Environment Agents, Intelligent Environment Repository and User Model interaction described in Figure 1. Both of these frameworks abstract information to make it available to users and the intelligent environment’s services whilst reducing the privacy concerns associated with using detailed information gathered in sensing environments. The abstraction of an information flow is a method of utilising information from a source that would otherwise infringe on the source’s privacy. This is considered in section 2.4.7.2.

2.3.2.3 Gaia OS

Pervasive computing environments suffer additional security risks as any users within the environment have access to its physical hardware. The Gaia OS is an intelligent environment architecture that was designed to address the inadequacies of traditional security in addressing the security concerns of pervasive computing, as physical and information security become interdependent and the physical risks to the environment become equally relevant (Campbell et al., 2002). The Gaia OS uses multiple authentication mechanisms to strike the balance between authentication strength and unobtrusiveness.

The Gaia OS uses Authentication Mechanism Modules (AMM) to implement authentication mechanisms independent of the devices used in the system, and Authentication Device Modules (ADM) for authentication that is device-dependent (e.g. use of biometric hardware). The ‘Mist’ communication infrastructure routes communications through an electronic cloud (or network) that disguises their origin and destination. It uses a hop-by-hop,
handle-based routing protocol that makes the tracing of communications by eavesdropping or untrusted third parties infeasible (Campbell et al., 2002). Combining this routing with limited public-key encryption allows data packets to be successfully routed whilst providing the user with improved privacy and concealment (Al-Muhtadi, Campbell, Kapadia, Mickunas and Yi, 2002).

The Mist infrastructure works by encrypting a message and its destination with the selected router’s public key and sending the message to the router. Once there, the message is decrypted and delivered to its destination (either to its ultimate destination or to another router for forwarding). The greater the required privacy, or perceived risk, the more routers need to be used to obfuscate the origin and destination of the message. The use of Mist routers requires the user to register with a central system, which keeps track of what users are logged onto a system and how they can be contacted. Collection of user information at this point could be considered a privacy risk and should be considered when being integrated into an intelligent environment.

The developers of the Gaia OS urge us to rethink traditional security in pervasive computing environments. Security in these systems must be considered from the start, not as an add-on later, and the scalable, distributed and physically accessible nature of these environments must be acknowledged (Campbell et al., 2002). Security must be scalable, multi-layered, and there should be some provision to build context-awareness into security policies (e.g. with permissions limited to temporally-based and location-based access). This approach to security is integrated into the dissertation’s interaction architecture to provide users with anonymous communication and information security.

2.3.2.4 MyPlace Intelligent Environment

MyPlace (Carmichael, Kay & Kummerfeld, 2005) is a prototype ubiquitous computing environment that seeks to overcome the invisibility problem plaguing intelligent environments that struggle with conflicting goals of being an unobtrusive service provider, whilst ensuring new users to the environment are informed of the available services. To overcome the invisibility problem (see section 2.3.5), MyPlace provides personalisation of the service’s interface in accordance with the user’s preferences and interaction history (stored on the user’s device). This interaction is represented in Figure 2

\[2\]

Figure 2 and Figure 3 were developed by the MyPlace authors (and not by the author of the dissertation), but were published along with the user study described in section 4.5.

Note: The author does not claim credit for the MyPlace system as a contribution made by this dissertation. The MyPlace Visualisation Interface (MVI) is used in the user study described in section 4.5, but contribution in this instance is limited to the user study results (and the resulting design requirements) described there.
MyPlace uses the accretion-resolution representation for modelling user’s and intelligent environment’s context (Carmichael, Kay & Kummerfeld, 2005). This system uses a combination of different sources of evidence, for example from sensors detecting activity, to build up a picture of the environment’s current context. The raw sensor data is transformed into evidence about the environment’s context, and then there is the accretion of this evidence to combine disparate signals and to weed out any conflicting information. The MyPlace system then resolves the information to interpret the environment’s current context whenever an application requires it. This is particularly useful for a system that collects a lot of information but may rarely need to resolve it.

Sensor information within this ubiquitous computing environment is published to the central server using a Publish-Subscribe messaging system (Segall, Bill, Arnold, Boot, Henderson and Phelps, 2000). Processes responsible for updating the model subscribe to these messages and update the model accordingly. The user’s personal device connects to the MyPlace server to access the service. Their personal device also holds their personal user model. They can also choose to release a portion of their personal user model, known as a persona, to the MyPlace server. The information in this persona is used to complement the model of the user that the MyPlace server has. More details on the MyPlace system can be found in (Carmichael, Kay & Kummerfeld, 2005; Kay, Kummerfeld & Carmichael, 2004).
The user and environmental models used in the MyPlace system are based upon the Personis user modelling system (Kay, Kummerfeld & Lauder, 2002). An example of this modelling is shown in Figure 3. In the example we can see the relationship between users, their devices and the environment’s places. The use of the accretion-resolution method allows information to be resolved only when needed, and it allows other privacy or security related restrictions to be put on the data. For example, the resolution (or accuracy) of a particular group of sensors could be lowered to improve users’ privacy or to offer them plausible deniability (Jiang & Landay, 2002), or access to a particular set of information (e.g. Kate’s location) could be restricted to a particular group or location.

![Figure 3: MyPlace World Model Example (Chatfield et al., 2005)](image)

The MyPlace interaction model raises some interesting questions. Where, for example, should the personalisation of the environment occur? Should it be located on the users’ device, for improved privacy, or on the MyPlace server for faster access times and reduced bandwidth load? The MyPlace system is used by the dissertation as a prototype to evaluate users’ interactions and privacy perceptions within intelligent environments. This user study can be found in section 4.5.

### 2.3.2.5 Personal Server

Intelligent environments normally utilise a personal mobile computing device (e.g. PDAs or mobile phones) to interact with the environment, store user information and interaction preferences, and to deliver ubiquitous computing services. The Personal Server is a mobile device that allows users to readily store and access the data and applications carried with the user and found around the environment (Want et al., 2002). This device has no display or input mechanisms, but relies on input and display devices found in public environments, and allows a user to carry their information with them. Ethnographic research has shown that users have access to several output devices (either shared or personal) about 70 per cent of the time (Consolvo & Walker, 2003). These devices include televisions, desktop computers, printers, laptop computers, PDAs and video projectors. This dissertation
therefore considers the Personal Server as a generic solution for providing client-side personalisation and management of user files and interaction preferences.

The Personal Server implementation is divided into three conceptual levels, each with specific research challenges: the user experience, the system infrastructure and the mobile platform. The system infrastructure in this case is required to facilitate the discovery process and to provide the interface and computation support for mobile users. The mobile platform itself is responsible for distributed file storage and remote control capabilities. The Personal Server uses LinuxOS and Bluetooth for connection with external networks, and provides significant storage capabilities that reverse the ‘thin-client’ paradigm traditionally used to provide services to mobile computers. This configuration allows storage and information manipulation to be controlled by the user, and the device is therefore referred to as a ‘user-controlled interaction device’.

The user-controlled interaction provides both advantages and disadvantages to using more traditional mobile computing to interact with intelligent environments. It allows users to maintain all their files and interaction preferences on a local device, reducing the bandwidth required for interacting with large data sets and improving security by not requiring the transmission of data via the Internet. This is obviously particularly important where Internet access may be unavailable or unreliable. The design also reduces power consumption and size by not using interface displays or input devices.

However, the user-controlled interaction device has some significant drawbacks. The Personal Server has minor problems with delays due to latency (especially during the Bluetooth discovery) and power consumption (Want et al., 2002) which, even without interface peripherals, is a persistent mobile device concern. Further privacy issues involve the use of public displays or with routing information through potentially untrustworthy third parties. The device is also discoverable via Bluetooth, leading the authors to suggest that a passive discovery process should be used only when a service is required (which require the users to access an interface to begin the service discovery process).

These current drawbacks may be overcome with effective system design, technological advances and user education. Socially based intervention might prevail on the use of public displays, or some security rules may evolve from detecting other users within the area and adapting the displays accordingly (Want et al., 2002). Other devices already carried could be co-opted into providing an interface to the user-controlled interaction device and its environment. As the computational ability of these devices increases, there will be increasing convergence of features as they are able to store and manipulate much more information.

A mobile phone, already carried by much of the population in developed countries, could double as a file storage and interaction interface. A watch display or hearing aid could double as a private output device. Better access to remote locations may also make the storage of information on mobile
devices irrelevant if the intelligent environment could access this information from a remote location in as timely and securely a manner. Any use of public displays for service interaction will require more research to assess the impact of these devices upon user privacy.

2.3.2.6 Privacy Sensing Ubiquitous Computing

A wide range of environmental conditions affect users’ privacy when interacting with intelligent environments. In order for users to understand the consequences of information exchanges or service utilisation within an intelligent environment, they must understand the local privacy policies, have access to personal information used and have a method of recourse if anything goes awry. The privacy awareness system (pawS) provides a method for announcing to users the data usage policies and provides a method for users to keep track of their personal information as it is stored, used and possibly removed from the system (Langheinrich, 2002). PawS allows users to remain informed about the consequences of sharing data within the environment and provides some accountability for the environment as users can receive reports on how the intelligent environment treats their personal information after it is exchanged. The pawS beacon provides local privacy policies in machine-readable form that can be parsed by the user’s mobile device and compared to the user’s privacy preferences.

A similar ubiquitous computing framework is the Confab privacy maintenance systems (Hong & Landay, 2004) that uses information tags to describe an application’s purpose, information collection activities and contextual or privacy information relevant to interacting with the system. These tags provide the users with feedback to enable them to more effectively consider the impact on their privacy when interacting with the environment. Confab is designed so that personal information wherever possible is processed and resides on the user’s mobile device.

The Confab system was further extended by Price et al. (2005) to add privacy legislation beacons to further enable users to react to changing contextual conditions. Intelligent environments could use similar beacons to provide information on services, the intelligent environment itself and any information that could be useful for users trying to determine the impact of an information exchange on their privacy. This information is examined in section 2.4 and is further considered in user studies described in chapter four.

Price et al.’s (2005) architecture utilises a negotiation between users’ personal preferences, local privacy laws and any environmental privacy policies. The authors further support the influence of social norms on the user by ensuring all information accessed (e.g. the users’ current location) is logged to support effective feedback on information usage, and by allowing users to insert noise into their personal information (reducing accuracy of information and increasing personal privacy). Noise in this case refers to Anonymising, Hashing, Cloaking, Blurring and outright fabrication of personal data to improve users’ privacy.
2.3.2.7 iCrafter Service Framework

iCrafter is a service framework for a class of ubiquitous computing environments known as interactive workspaces (Ponnekanti, Lee, Fox, Hanrahan and Winograd, 2001). This framework provides access to environmental hardware devices and software services through user interfaces (UIs) generated at the time of use. It seeks to provide adaptable, portable, ‘on-the-fly’ aggregation of ubiquitous services by using standard service descriptors and environmentally located intelligence to help select, generate and adapt service UIs (Ponnekanti et al., 2001). This focus on adaptability, deployability and aggregation highlights critical characteristics of ubiquitous computing environments.

Adaptability and deployability are important, as ubiquitous computing environments tend towards heterogeneous systems comprised of varied legacy systems and different hardware (in terms of OS, computational power and adaptability). An environment must be robust and allow the user to engage with the environment no matter their input device (OS, UI, etc.). It should also provide contextual relevant information services to help users develop associations between the services and their environment (Ponnekanti et al., 2001). The aggregation of service delivery is perhaps even more important as intelligent environments incrementally develop new services and add information sensors to existing infrastructure.

The iCrafter developers selected to develop interfaces as patterns, allowing one pattern to be utilised by a class of services or hardware (e.g. commands for all digital cameras) (Ponnekanti et al., 2001). iCrafter uses a flexible event-based communication platform to distribute (or publish) service descriptors to the environment. Service beacons use a lightweight extensible language (e.g. XML) to provide presence and descriptive information to the environment. Users wanting to use a service make a request to a central component (an Interface Manager), and it generates a UI based upon the available services, its generic interface patterns, the output device and any relevant contextual information. Users then use this UI to send interaction requests to the associated hardware or software services.

iCrafter has many strengths which can be exploited as part of a greater ubiquitous computing ecosystem. It places intelligence in the ubiquitous environment to select, generate and adapt services to a particular UI. It provides extensibility and better handling of legacy services and resource-limited appliances, which improves the ability of the environment to handle a whole lifecycle of service development, from creation through to supporting old unsupported services that may still have useful functionality. iCrafter also provides ‘on the fly’ service aggregation and creates context-aware UIs that are portable across workspaces (Ponnekanti et al., 2001).

2.3.3 Context Awareness

Context is any information that can be used to describe the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves (Dey, 2001).
Context awareness describes the making use of contextual data (either sensed directly or provided by the user or a sub-system) to increase the richness of communication between users and the environment, and to make it possible to produce more useful services (Dey, 2001). The use of context within an intelligent environment allows the environment's services to represent and react to the current state of the environment and (ideally) allows the user (or their device) to critically question the state of the environment (Ulrich, 2008, pg. 8). The current context can have a great influence upon information exchanged, and can drastically affect the user's view of privacy within the intelligent environment (Lederer, Dey & Mankoff, 2002). How intelligent environments collect, utilise, store and disseminate this context information (including information about the system’s users and their devices) not only determines how effective its services are, but also determines their impact on the users’ privacy and information security.

Intelligent environments are able to develop a sense of what is happening in the environment by the collection of data from multiple sources. External systems and users themselves can provide information via personal preferences or specific user accounts, information can be inferred from the user’s activities or actions, or it can be collected directly by numerous environmental sensors. These sensors are typically computationally simple, collect only a specific type of information and can be used with varying levels of accuracy. Varying the accuracy of the information provided by sensors or other information sources can have huge implications for users’ privacy. This is discussed in more detail in section 2.4.7.2, including methods of utilising this data whilst enhancing user privacy.

Context information includes spatial (location, speed), identity (of the user and anyone else in the vicinity), user model (profile, preferences), temporal (time of day or year), environmental (noise, light), social (meeting, party), resources (printers, fax, wireless access), computing (network bandwidth, login), physiological (hearing, heart rate), activity (supervision, interview), schedules and agendas (Chen & Kotz, 2000; Dey, 2001; Korkea-aho, 2000; Leonhardt, 1998; Salber, Dey, Orr and Abowd, 1999). Contextual information could also include information that cannot be sensed by the environment, but is instead provided by the user or their device. Ulrich (2008) identifies a user’s motivational and moral context as important influences on a user’s actions, and any ubiquitous computing interaction should allow the user’s current motivations and interaction desires to influence interaction decisions. The user’s motivational or moral context is unlikely to be provided to the intelligent environment, but instead is likely to be used to personalise service delivery on the user’s mobile device.

It is the capture of this contextual information that makes intelligent environments both so useful and so dangerous to users’ privacy. The personalisation of ubiquitous computing services based upon user-provided or environmentally-sensed information improves the service’s usability and value, but the storage, management and dissemination of this information can lead to grave privacy violations. These threats to privacy have led to a call for the use of these sensing devices only in specially defined areas (e.g.
emergency rooms, aircraft hangars, etc.) (Langheinrich, 2002), and underlines that the dissertation’s architecture must be able to provide services without environmental surveillance.

Context is a dynamic construct (Greenberg, 2001) that allows services to be tailored to current environmental conditions and provides users with the ability to personalise their interactions to react to varying environmental conditions. Context recognition is required before a mobile device may make decisions for a user within an intelligent environment. The sensing of user activities, available intelligent environment infrastructure and the physical context is essential for the adoption of context-specific identities (Jendricke, Kreutzer & Zugenmaier, 2002). Effective interaction management requires an interface (or decision engine) that can take into account the user’s moral and motivational context in its evaluation of required service interactions. This user information would most accurately be provided directly.

Iachello, Smith et al. (2005) recently investigated information sharing using a peer-to-peer, mobile, location-enhanced messaging service. The exchange of location-based contextual information between participants through automatic and user-initiated messages compelled users to consider how they would like to share information about themselves. The study found that automated messages were not required or desired by the participants, and suggests that automatic information sharing should be minimised or eliminated within ubiquitous computing environments (Iachello et al., 2005). This is investigated in section 4.2.

The information sharing study also found users often provided false or sufficiently general information to other participants to allow a form of plausible deniability on location and contextual information (Iachello et al., 2005). This deliberate misrepresentation (similar to telling social ‘white lies’) mirrors a pervasive problem in context-aware systems, as contextual information can often be incomplete or incorrect. This ability to control what information is shared is essentially how users maintain their privacy in real life. Tools that support user interaction must allow them to represent themselves to the environment and other users however they wish, including interacting anonymously.

The ability of ubiquitous computing system to be situated within an existing environment allows the collection and use of context in tailoring services and their delivery. Whilst this provides great potential for the delivery of personalised, useful, environmentally reactive services, it also causes great concerns for the casual user. With increasing concern over unauthorised or unnoticed collection of user information, the use of contextual information in ubiquitous computing environments must be evaluated. Methods of privately collecting and using personal information to allow users access to the benefits of personalised service delivery is discussed in section 2.3.5.

### 2.3.4 Knowledge Representation

Knowledge representation is a multi-disciplinary subject that describes the definition and storage of knowledge. This field is a combination of Logic
(providing the formal structure and rules of inference), Ontology (defining the kinds of things that exist in the application domain) and Computation (the application of the knowledge into computing systems) (Sowa, 2000). Ontology languages allow users to write explicit, formal conceptualisations of domain models. The main requirements of these languages include well-defined syntax and semantics, efficient reasoning support, and sufficient expressive power and convenience of expression (Antoniou & Harmelen, 2003). Ontological knowledge includes class membership, equivalence of classes, consistency in knowledge representation and the ability to classify knowledge.

Semantic networks have been identified as a method of representing an intelligent environment’s context (Peters & Shrobe, 2002). Semantic networks use associations to create links describing different knowledge about the intelligent environment’s physical environment. They are a prerequisite for reasoning support, allowing derivations to be made mechanically instead of by hand. This improves the consistency of the ontology and knowledge, helps check for unintended relationships between classes and allows for the automatic classification of instances in classes (Antoniou & Harmelen, 2003).

Semantic networks have been used for years to represent knowledge in artificial intelligence systems (e.g. A is part-of B), and can effectively record user information, provide meeting and resource management, and describe location infrastructure (Peters & Shrobe, 2002). This notation allows the relationship between user data, contextual information and physical locations to be effectively represented (e.g. Room 832 is part-of the 8th Floor, which is part-of Building X). A simple representation of part of a semantic network is described in Figure 4.

![Semantic Network Representation](Peters & Shrobe, 2002)

Web Ontology Language (OWL) is a multi-tiered ontology that attempts to provide a standardised and broadly accepted ontology language for the Semantic Web (Antoniou & Harmelen, 2003). OWL uses XML-based syntax to define knowledge, relationships between information and its attributes etc. There are three versions of OWL, each allowing different levels of expression and reasoning about a body of knowledge. The full version of OWL allows control over information relationship cardinality, providing the ability to limit classes and reasoning behaviour, and support for previous ontological languages (e.g. RDF). The OWL DL (description language) and OWL Lite subsets restrict the way in which constructors can be used, reducing the
language’s extensibility but providing more efficient reasoning support (Antoniou & Harmelen, 2003). Similar semantic ontology languages have been developed for more specific purposes, especially in ubiquitous computing, to improve reasoning efficiency and to increase usability.

The Accretion model (Kay, Kummerfeld & Lauder, 2003) provides a similar scheme for the standardised sharing of user and environmental information within intelligent environments. It allows users complete control over their personal information through the use of multiple user models, and these models control the personalisation of an interface within a ubiquitous computing environment. It distinguishes knowledge, beliefs, preferences and other attributes of the user, including their personal attributes such as names, height, date of birth and other arbitrary aspects, such as their location. This model is an extension of the Personis user model (Kay, Kummerfeld & Lauder, 2002), which was based upon previous User Modelling (UM) Languages.

The advantage of this system is that it is very clear in describing how information is being used, which data is more reliable than others, and to ensure external entities have access to appropriate data (Kay, Kummerfeld & Lauder, 2002). The use of data in this way (e.g. X is more reliable than Y, Z only has access to Y, etc.) makes things clearer to people using the system, and allows for increased user confidence. The accretion model reinforces the need for the system to acknowledge that there may be inconsistencies in the data and in the system’s knowledge. It is important to recognise that the different ways of assessing stored information are crucial to the effective use of the system.

The accretion architecture is distributed, ensuring appropriate access to information. For example, most applications will not have access to location information, while the application that tracks location may not have access to the sensors in your home (to ensure privacy while at home) (Kay, Kummerfeld & Lauder, 2002). There are several levels of such access control in the accretion representation:

- Evidence sources
- Component
- View
- Context

By using ‘resolvers’ to examine data, more effective data measures can be added later without affecting the data source (the data is examined through resolvers, the resolvers do not change the data) (Kay, Kummerfeld & Lauder, 2002). The system also uses ‘justifiers’ to explain why a particular personalisation or information filtering occurred, and the visibility that these provide to the user is extremely important (Kay, Kummerfeld & Lauder, 2002). The use of this representation of the system’s actions opposes the view that ubiquitous computing systems should be invisible. The balance between when users can interact and have a sense of control over the intelligent environment, and the desire to have these environments operating in the background below our conscious awareness is a compromise that
needs to be reached. This is described as the invisibility problem and is discussed in more detail in section 2.3.5.

Other user modelling languages are being developed using XML. The UserML markup language is an XML-based exchange language, which is based upon an ontology that defines the semantics of the XML vocabulary (UserOL). This language was designed to create user models of ubiquitous computing environments. This method for creating partial user models, which could be used across multiple ubiquitous computing environments (Heckmann, 2003), mirrors the efforts of the Personis (Kay, Kummerfeld & Lauder, 2002) and Accretion models (Kay, Kummerfeld & Lauder, 2003) to allow effective communication between users and intelligent environments. iCrafter also uses a similar modelling language for its service descriptions (Ponnekanti et al., 2001).

Heckmann’s (2003) approach identifies two different levels. The first level offers a simple XML structure for all entries of the partial user model. These UserData elements consist of category, range and value fields (Heckmann, 2003). The second level reveals the ontology that defines the categories. The advantage of this approach is that different ontologies can be used with the same UserML tools. Thus different user modelling applications could use the same framework and keep their individual user model elements (Heckmann, 2003). The use of distributed partial user models is also examined by Kay, Kummerfeld and Lauder (2003).

The Security Assertion Markup Language (SAML) is an OASIS standard (OASIS, 2009) that is uses XML-based notation to describe and communicate security credentials and other information (e.g. asserting user identity) between entities. The OASIS SAML standard defines precise syntax and rules for requesting, creating, communicating, and using these SAML assertions. SAML is used in the Shibboleth architecture (Shibboleth, 2005) and Liberty Alliance Web Services Framework (Liberty Alliance, 2002) to provide a single sign-on and attribute exchange framework. Shibboleth extends the SAML model to include the notions of attribute release policies (from the identity provider) to address privacy issues and attribute acceptance policies at the destination to address semantic trust issues (Shibboleth, 2005).

Semantic networks allow a great deal of flexibility in terms of the data they can capture and interpret. The nature of the semantic networks means that adding and changing information is localised and clear-cut, and inferences of information can be generated extremely efficiently (Peters & Shrobe, 2002). The separation of knowledge and inferences about that knowledge allows effective security and privacy safeguards to be built into the knowledge base, preventing the movement or use of knowledge that would influence the user’s privacy or security. The specific ontology used, e.g. OWL, Accretion Model, UserML, etc., determines the trade-off between the complexity of knowledge represented versus the required reasoning speed. These languages all identify the benefits of using XML notation to share information that can be rapidly reused between systems.
Further work has been done describing methods for securely distributing information within an intelligent environment. Hitchens, Kay and Kummerfeld described a method of using third parties to provide user model templates for information sharing (Hitchens, Kay & Kummerfeld, 2004). Users obtain a model template and have a third party sign the information in their template as true and correct. Users can then share any part of the user model with the environment, without needing to provide further identifying information. The template used in the exchange could easily be made known to the service provider to improve the processing of the information exchange.

This provides an additional method for the intelligent environment to authenticate information asserted by the user, even when limited information is provided, for example when the user simply presents their age. As the information is signed by the third party, the system can now consider whether to trust the third party or reject the data. The use of trusted third parties can therefore allow users to share only the information about themselves that they wish, protecting their privacy by allowing the desired level of anonymity.

This method of sharing partial user information templates is integrated into our intelligent environment architecture. This system and its support of user anonymity and pseudo-anonymity are further described in section 2.4.5.1.

2.3.5 Personalisation

Personalisation is the act of tailoring an interface or relationship based upon users’ known or anticipated preferences to provide a better service or user experience. Personalisation is normally achieved using an existing user profile or persona describing the user and their preferences. A user persona is a collection of data stored in a record designed to be rich enough to provide the record-holder with an adequate image of the represented identity (Clarke, 1994). Users will likely have multiple personae, each for a different interaction purpose (or to reflect a separate aspect of their identity). Personae are considered in more detail in section 2.4.4. A user profile is conventionally used to refer to the small set of data that reflects the user’s interaction preferences. The information stored on a user profile could also logically be stored on a user’s persona for reuse in similar services.

Two methods exist for acquiring a user profile for personalisation: asking the user (profiles, questionnaires etc.) and watching the user (click-stream or transaction analysis) (Koch, 2002). Problems with these are that users often do not trust the personalisation system (in collecting data about them), and the fact that many systems require lots of data before useful suggestions can be made (the ‘cold start’ problem). Koch suggests the use of personal profiles to allow users to store and maintain the information, to address the trust issues and allow more information to be used initially and therefore avoid the ‘cold start’ problem (Koch, 2002). A user profile could be generated from the information provided on a specific user persona.

Personalisation can also be based upon user location and other environmental context. BlueStar (Quigley, Ward, Ottrey, Cutting and Kummerfeld, 2004) is a privacy-centric location-aware system to allow users to access location information without requiring them to identify their location to the central
server. BlueStar downloads wide-area location information to the users’ handheld device and personalises this information based upon their exact location (which is only known by the mobile device). This type of client-side personalisation allows the users personalised service delivery without requiring them to give up valuable personal information (in this case their exact location).

The use of personae or user profiles in tailoring services and interfaces within intelligent environments raises several concerns. Users want control over the collection and reuse of their personal information, but still want a simple and efficient method of interacting with intelligent environments with potentially large numbers of services. The management of users’ identity, discussed in section 2.4.4, investigates how users can derive the benefits of tailored information service delivery while satisfying their need for privacy. The dissertation also investigates the challenge of balancing the goals of invisibility with the need for accessibility.

The invisibility problem describes the conflicting goals of ensuring ubiquitous computing blends naturally into the background (Weiser, 1991)with the need to draw the attention of users to its services. Intelligent environments are supposed to include calm technologies that blend into the environment, allowing services to be ‘invisible’ when not being utilised by the user. For example, an environment might contain a number of information services that can be provided to the user’s mobile device, but would be invisible to users without the correct hardware. An augmented household mirror might provide a reminders or message space for members of the household, but would seem to be an ordinary mirror to household guests (Chatfield et al., 2005).

The invisibility problem raises a number of questions. How do new users locate and learn to use these services? Suppose the household guest entering this intelligent home environment is a relative who is coming to stay for a few months. How can we provide information about this person to the intelligent environment so that they are treated like a member of the family and given access to the interactive facilities? Invisibility of environmental services and context can also prevent users from critically questioning the environment around them (Ulrich, 2008), and therefore must be avoided where possible.

There has been some exploration of ways to address aspects of the first form of invisibility. Heer and Khooshabeh examine invisibility from a psychological perspective, making the point that an invisible interface does not in any way imply physical invisibility (Heer & Khooshabeh, 2004). The Digiscope (Ferscha & Keller, 2003) explores the use of augmented reality: it provides a large semitransparent window to view the world. Visual tag recognition and RFID are used to detect items in a suitcase, and the display shows information about items within the suitcase. Other approaches have explored using fiducial markers to augment the environment, delivering information through a mobile phone which recognises the markers by using a camera (Assad, Carmichael, Cutting and Hudson, 2003; Rekimoto & Ayatsuka, 2000). These systems require the user to point a device at the right part of the intelligent environment to receive information on the environment. If the user were
unaware of a service in the environment, they would not be able to use this class of interface.

A quite different dimension of invisibility relates to the automatic and natural use of facilities in the intelligent environment as envisaged by Weiser (1991). The challenge in this case is that an artefact which is natural to use for the experienced user requires learning for the new user. For example, an experienced user of a microwave oven is barely aware of the steps in making normal use of it, yet the first-time user takes some time to work out just what to do (Chatfield et al., 2005). The same will apply for communication with an intelligent environment. When users first meet a new part of an intelligent environment, they may well appreciate personalised information about the device and benefit from tuition and assistance to master it. This is a candidate for personalised tuition (Brusilovsky, 2001).

These problems indicate that a standardised method of accessing intelligent environments might be necessary. Users are unlikely to be willing to learn new methods of interaction for each of the multitude of intelligent environments that are likely to begin to invade their everyday lives in the near future. A pervasive, widely accepted intelligent environment architecture will require a standard interface for accessing services and a method of privately personalising this interface and any service interaction based upon the user’s preferences and usage history.

### 2.3.6 Service Discovery

Service discovery is the process of publishing details of a service so that clients can then search and discover any services that meet their requirements (Turner, Budgen & Brereton, 2003). In ubiquitous computing this process is normally limited to the surrounding environment, using wireless transmission of service beacons. Service discovery is the mechanism that allows services to be used on demand without prior arrangement, allowing users to discover services that they were previously unaware of. It involves the distribution of a service description describing the service and how to access it. The services are delivered through three layers:

- The service transport layer (or the network layer) that handles the communication between all parties;
- The service integration layer, which manages the negotiation and service discovery between the user and the services provider; and
- The service layer, which hosts the services and delivers them to the user via the service transport layer.

An architecture looking to provide ad-hoc or on-demand services across a network must provide this functionality. The delivery of software in this manner is commonly referred to as ‘Software as a Service’ (SaaS).

Three protocols have become so widespread that they are synonymous with Web services. These include Simple Object Access Protocol (SOAP) (to provide message format for communication with the service), Web Service Description Language (WSDL) (describing how to access the service) and Universal Description, Discovery and Integration (UDDI) (which provides a
register of services that clients can search) (Turner, Budgen & Brereton, 2003). The protocols used to distribute service descriptions (also called Service Beacons (Ponnekanti et al., 2001)) are less important than their characteristics. Communications must be private, secure between the user and service, and discoverable within a certain environment (such as the local ubiquitous computing environment or across the Internet).

The majority of service descriptions use an XML Schema language to describe the service (Turner, Budgen & Brereton, 2003). The schema used should be lightweight and extendable to allow for the customisation of the service description and discovery process. Example schemas are described in section 2.3.4. iCrafter uses XML descriptors that are broadcast from service providers and stored in a central location that users entering the environment check (in this case the ‘event heap’ or interface manager) (Ponnekanti et al., 2001). This provides a robust method to allow users to discover available services, and in this case provides generic user interfaces for their use.

A secure service discovery service, which provides encrypted communication and meta-data descriptions to direct service discovery, is described in (Czerwinski, Zhao, Hodes, Joseph and Katz, 1999). Other methods of broadcasting services would include Elvin, mDNS or similar simple servicer registers. The method selected would depend on privacy considerations, whether a central service or interface list is desirable, and how often the services in a given environment would vary. iCrafter’s provision of generic interfaces might also be preferable for services that are difficult to provision with standard interaction tools (e.g. using a html browser, etc.).

2.3.6.1 Service Oriented Computing

Service Orientated Computing (SOC) is a computing paradigm that utilises services as fundamental elements for developing a solution (Papazoglou, 2003). Services are self-describing, platform-agnostic computational elements that support rapid, low-cost composition of distributed applications. These services can range from simple calculations and requests to complicated business processes. The SOC services allow organisations to expose their core competencies programmatically over the Internet using standard (XML-based) languages and protocols, and to be implemented via a self-describing interface based upon open standards (Papazoglou, 2003). SOC or Service Oriented Architecture (SOA) is a logical extension of SaaS. It not only provides distributed service delivery but also allows for dynamic discovery and binding of services when they are required. This allows customers to access services without pre-existing arrangements and without signing up to ongoing licensing fees or making large upfront payments.

These services are technology neutral, loosely coupled and support location transparency to allow the running of the services irrespective of their location or delivery platform. Services can be stand-alone or can be combined into composite services to produce more complex functionality. Service Providers publish their services on a Service Registry which clients use to find and connect to services (Papazoglou, 2003). Services are traded on a common marketplace specific to a particular industry or geographical area (e.g. ERP
services marketplace). The marketplace is created and maintained by a ‘market-maker’ (potentially a consortium of organisations) that brings suppliers and vendors together. The market-maker assumes responsibility for marketplace administration and performs maintenance tasks to ensure the administration is open for business (Papazoglou & Georgakopoulos, 2003).

The Extended SOA (ESOA) describes the role of Service Aggregators and market regulators in managing the marketplace (Papazoglou & Georgakopoulos, 2003). Service Aggregators combine basic services into composite services, which are then published on the SOA. They develop specifications and/or codes that enable coordination, monitoring, conformance and Quality of Service (QOS) composition management for the composite services. The market administration provides access to managed composite services that provide operational assistance (ensuring access and providing support) and market governance (including service certification, ratings and Service Level Agreements) (Papazoglou & Georgakopoulos, 2003).

SOC is in many ways similar to services provided in ubiquitous computing environments. Services are developed to be used independently of pre-existing relationships and support ad-hoc use (allowing them to be combined into greater services comprised of disparate smaller services). Ubiquitous computing services, therefore, need a method of advertising themselves to the environment, and a cohesive integration infrastructure that allows the exchange of identity information and governing behavioural statements (QOS, expectations of privacy etc.).

2.3.6.2 Ubiquitous Computing Services

Ubiquitous computing services are largely independent of an intelligent environment’s architecture. Gunter et al. (2004) present four scenarios similar to those proposed in other work: FriendsinTown.com, What’s Here?, Market Models and Travel Archive. FriendsinTown.com describes an alerting service in which users are alerted to a specific event within their current environment (e.g. a friend is nearby or an event is taking place). The What’s Here? service provides the user with environmental information that might be personalised in accordance with the user’s preferences (e.g. forthcoming group meetings or events). Market Models describe an environment at a given time (e.g. how many users were logged in at 2pm Friday). The Travel Archive service records information on the user’s activities and can be used to ask time- or location-based queries (e.g. ‘Where was I on Sunday at 1pm?’).

These services demonstrate the two main types of ubiquitous computing services: real-time services and historical services. Historical services are interesting when considering users’ perceptions of information storage and re-use. Real-time services are interesting when considering user interaction, privacy and information usage. Real-time services can further be categorised into ‘Interrupt-Based, where the user is alerted once a certain criteria is satisfied, and Query-Based, where the user asks for information based upon their current location’ (Price, Adam & Nuseibeh, 2005).
A ubiquitous computing architecture requires an interaction method that makes these services possible without endangering the user’s privacy and security. The architecture must therefore include protocols for service discovery and information exchange, and the ability to conduct anonymous and/or personalised interactions with the environment and service provider. The services that our ubiquitous computing infrastructure supports, and the necessary support entities, are discussed in section 5.2.2. This section is informed by the results of the User Studies in sections 4.2, 4.3 and 4.5.

2.3.7 Summary and Conclusions

Intelligent environment development has matured to the point where interaction with environments and services is well understood, and numerous user interfaces and models of user interaction have been suggested. This research, however, challenges the architectures featured in section 2.3 as being inadequate for securing user privacy whilst providing all the interactions that are required in intelligent environments. The abstractions of information and service delivery described in the Merino Architecture and the Framework for Intelligent Instrumented Environment do not consider interaction with multiple environments or consider personalisation of service delivery for different interaction goals.

Other intelligent environments provide useful methods of securing user privacy, storing information within intelligent environments, and examine the user feedback required for users’ understanding of the impacts of an interaction on their privacy. These intelligent environments do not provide a complete interaction solution, especially when considering the overlap of multiple intelligent environments. The environments in section 2.3.2 form the basis for the dissertation’s evaluation of intelligent environments, and are combined into a new intelligent environment architecture that addresses these shortcomings. This architecture will incorporate the requirements of personalised service delivery, described in section 2.3, and will include privacy and security design requirements identified later in this chapter.

Contextual awareness is one of the chief benefits to utilising an intelligent environment’s services. These services have the ability to adjust their service delivery to changing conditions within the environment. Combined with an interaction persona (or user profile) the services can be personalised to improve service delivery and enhance the overall experience of interaction with the intelligent environment. Contextual data, combined with interaction persona (or user profiles), can improve service delivery and greatly enhance the overall experience of interacting with the intelligent environment. But users must be able to make a determination on what information is being collected on/from them and what the benefit versus risks to their privacy they face.

Intelligent environments should not automatically use sensors for identification purposes, nor should they automatically share this information with other users, environments or services. The use of environment monitoring sensors should be clearly communicated to the users when they enter the environment. Data collection and storage in the environment must
also be planned so that stored data does not overtly impact on the user’s privacy (even when such collection is advertised). Varying the accuracy, timeliness and type of contextual information stored can have large impacts on the user’s privacy, so only the minimum amount of information required for service personalisation should be collected and stored.

All information stored within an intelligent environment should use an easily accessible notation standard that can be integrated into different services. The SAML identity assertion notation is a standard method of providing identity assertions to an intelligent environment. Information stored within the environment should where possible be kept separate from basic personal information observed or gathered from the user. This allows better visibility of system data, improves the user's understanding of the use of information within intelligent environments, and helps separate the security and privacy requirements of sensed, provided and inferred user information. Personae are user controlled representations of an aspect of their identity. Personae can be exchanged with intelligent environments and other users to provide identity information or to personalise service delivery.

Personalisation within an intelligent environment is essential to help users navigate the potentially huge number of services available in any given environment (i.e. particularly if there are multiple intelligent environments serving an area). Personalisation helps not only to tailor services (and their interfaces) to the user’s preferences, but it also provides a means of maintaining the right balance of invisibility and service visibility. Personalisation can occur at the system level or the device level, with the trade-off of providing more personal information to the system to reduce the size of interface downloaded to the user’s mobile device. While both of these methods are valid design decisions, the dissertation’s focus on maintaining user privacy will likely mean that personalisation will mostly occur on the user’s mobile device (as demonstrated in (Quigley et al., 2004; Want et al., 2002) and section 2.3.5).

### 2.4 Privacy

Privacy is the interest that individuals have in sustaining a ‘personal space’, free from interference by other people and organisations. (Morison, 1973)

Users are becoming increasingly concerned about their privacy, both over the Internet (Kobsa, 2001; Patrick & Kenny, 2003), and within intelligent environments (Langheinrich, 2001). But what is privacy? Justices Warren and Brandeis (1890) were amongst the first to qualify privacy in common law, and identified that all citizens have an intrinsic ‘right to be left alone’ or freedom from intrusive press, fellow citizens or modern capture or recording devices. The authors argued this based upon their belief that common laws already secured ‘to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others’ (Warren & Brandeis, 1890).

The definition of provided by Morison (Morison, 1973) describes privacy as an interest, rather than a right. This privacy interest covers a number of areas,
including the privacy of person, privacy of personal behaviour, privacy of personal communications, and privacy of personal data. Information privacy describes the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves (Clarke, 2000). This is especially relevant in this dissertation as the interaction with intelligent environments and their services is primarily concerned with what information is collected, stored and used to provide personalised services. Each of the privacy areas covered by the above definition are of concern, but intelligent environment (compared to more normal information systems) has the ability to collect information on the user’s behaviour through sensing their movements and the potential collection of surveillance information.

Clarke (Clarke, 2000) expands the definition of information privacy to consider the complex nature of privacy itself and the interactions between competing interests. Privacy protection is a process of finding the appropriate balance between privacy and multiple competing interests. This is especially important for this dissertation. Intelligent environments provide countless methods of breaching the user’s privacy. Personalised service delivery in intelligent environments is essentially the exchange of information in return for a service of perceived value. This dissertation must therefore consider the interaction between service delivery and privacy, and will develop an architecture that provides as much privacy protections as possible.

An extensive analysis of privacy and privacy protection is provided in (Clarke, 2000). Historical and philosophical discussions of privacy can be found in Flaherty (1972), Seipp (1981), Schoeman (1984), Smith (1997), Burkert (1999) and Bennet & Grant (1999). Westin (1967, p. 31) describes the nature of users’ privacy by examining the four basic states of user privacy: solitude, intimacy, anonymity and reserve. Any environment that seeks to support users’ privacy in a natural manner must allow users these methods of interaction. Environments must not intrude on users’ solitude, must provide connections to intimate friends and family, allow anonymous access to services, and allow users to determine how much information (if any) they wish to share with the intelligent environment.

Westin’s work was later integrated into the Fair Information Practices (FIP) legislation which defined rules surrounding information privacy to ensure interoperability of systems designed to share personal data. The school of thought grounded in the FIP, legitimised by Westin’s publications, was that ‘the invisible hand of business and government activity would ensure that IT did not result in excessive privacy invasion’ and hence privacy regulation is unnecessary (Clarke, 2000). The OECD, concerned that a proliferation of varied privacy protection laws might harm economic growth by creating accidental trade barriers, codified the FIP-based regime in the OECD Guidelines (Clarke, 1998a). (See section 2.4.1 for more on the OECD Guidelines and evolution of privacy regulation). Definitions of privacy are increasingly being adapted

Definitions of privacy are increasingly being adapted to the information age as society evolves what it considers as acceptable behaviour and as technology changes what invasions of privacy are possible. Warren and Brandeis’ view of
privacy has evolved into the ‘protection against unreasonable or burdensome intrusions’ (Lessig, 1999, p. 148), or the act of keeping information secret from all but those who are authorised to see it (Menezes, van Oorschot & Vanstone, 1996). These definitions are increasingly centring on the capture, storage and protection of personal information.

Most modern privacy laws address information privacy, but information privacy is not the only type of privacy threatened. Intelligent environment’s ability to collect location and locational habits can threaten the user’s personal security by exposing their whereabouts to interested third parties. Privacy of behaviour is threatened by the surveillance aspects of ubiquitous computing. A holistic solution should also consider privacy of the person, which describes the freedom from compulsory immunisation or blood transfusions, the privacy of a person’s genetic makeup (protecting a person’s DNA or tissue samples) and the ability of people to make their own decisions involving the integrity of their body.

Langheinrich drew on Westin’s work (and the FIP) when developing his Principles for Privacy Aware Ubiquitous Computing (Langheinrich, 2001). While these principles provides a basis improving user privacy when interacting with intelligent environments, they contain the same focus on promoting clear information exchange and allowing users to manage this information flow, instead of adopting a more wide reaching view of personal privacy. Privacy solutions solely based upon this limited view of information privacy cannot satisfy users wider definition of privacy, cannot satisfy data EU protection laws, and will not be effective.

Intelligent environments proposed by researchers describe systems that incorporate unprecedented levels of information gathering in all areas of our lives (Lahlou, Langheinrich & Röcker, 2005), and the need for user privacy controls in these environments is well established (Bellotti & Sellen, 1993). The risks associated with ignoring the role of privacy in the development of new pervasive technologies are significant. Each new technology brings with it new concerns about the capture, use and storage of personal information, and the consequences of ignoring these concerns have ranged from receiving burdensome unsolicited e-mail (e.g. SPAM) or telephone calls during dinner (Price, et al., 2003), to the deaths of hundreds of thousands in extermination camps (Black, 2001). Privacy is not only a legal right, affording protection to persecuted minorities, but is also an essential element in the operation of individuals, groups, and government in a democratic society (Westin, 1967, p. 368). Privacy therefore is not only essential to the successful development of usable intelligent environments, but any system that seeks to erode personal and organisational privacy would be detrimental to society as a whole, and is likely to be rejected by users en masse.

Intelligent environments automate the collection of personal data and the tracking of a user’s location or activities. This collection of information is often done invisibly, without the user’s knowledge. These systems are eroding natural boundaries of privacy and are an increasing concern for their users. These dangers to user privacy have been shown to be the biggest obstruction to the successful development of intelligent environments (Jiang, Hong &
Landay, 2002; Kenny & Borking, 2002; Langheinrich, 2001). Users must be protected from unreasonable surveillance and recording of personal activities if intelligent environments are to be successfully implemented and accepted by users, and therefore available to support users with useful services.

Privacy is an increasingly more fluid concept that is defined by the context of the exchange and influenced by the perceived risks and benefits of sharing information at any given moment (Kenny & Borking, 2002; Lederer, Dey & Mankoff, 2002). Maintaining users’ privacy must acknowledge the dynamic nature of privacy, and allow the judgement of the privacy risks associated with an information flow to be made dynamically, either by the user or on their behalf. Users must have control over their information or pass this control to a third party, like a dynamic trust or reputation system described further in section 2.4.6.

MIT professor Gary Marx believes the source of outrage against surveillance is its ability to cross personal borders of privacy (Marx, 2001b). These personal borders are natural borders of privacy (e.g. walls, envelopes etc.), social borders (e.g. expectations of professional or personal discretion), spatial or temporal borders (e.g. separation between different periods of one’s life) and ephemeral or transitory borders (e.g. expectation that personal interactions or communications and remnants such as garbage are not captured and stored). Surveillance crosses these borders and allows information that should be private to be made available in different environments or settings.

These natural borders of privacy provide valuable guidelines when considering the collection and storage of information. Intelligent environments must respect these personal borders and prevent information flow across them to ensure that the environment has no negative impact on personal privacy (Langheinrich, 2002). Intelligent environments need to have clearly defined boundaries that limit information collection, and clear guidelines on the sharing of information across these boundaries that users can agree on.

Managing the flow of information and its impact on user privacy is both a social and technical matter. Users that have limited understandings of how information is shared via a computing system may inadvertently expose more information than they would in a similar real-life situation. Technical security products like firewalls or password login systems often overstate their protective capabilities and are vulnerable to social attacks (see section 2.5.2.3). This leads to difficulties in users understanding how they can manage their privacy and reduces overall trust in new systems. Systems designed to maintain user privacy must not only address technical security, but also need to clearly show how and to whom information is distributed, and need to make users aware of the potential risks to their information (and therefore privacy).

Privacy is a social notion shaped by culturally determined expectations and perceptions about one’s environment (Bellotti & Sellen, 1993). Expectations of privacy differ between different cultural groups, and with experience with sensing technologies. The social nature of privacy must be considered to effectively maintain and promote user privacy within ubiquitous computing
environments (Bellotti & Sellen, 1993; Jiang, Hong & Landay, 2002; Kobsa, 2001; Langheinrich, 2001; Langheinrich, 2002; Lessig, 1999; Weiser, 1993). This is especially relevant due to the social nature of many ubiquitous computing services. Many services provide location and presence information to other users, store information about the user and their service habits (to personalise their subsequent service experiences) and could potentially be used to create a very detailed picture of the user’s life.

The types of information collected by sensors and stored within an intelligent environment is important. Surveys since the 1970s show that loss of privacy is associated with the quantity of personal information collected, and that fear of privacy infringements constantly increases with the integration of computers in everyday life (Robbin, 2001). Data representing the same content can be acquired with different levels of confidence, transferred at varying degrees of accuracy, and exists for different periods of time. Each of these factors have varying implications for privacy (Jiang, Hong & Landay, 2002). Intelligent environments must be designed to collect the minimum information necessary to provide a service, and where possible should be stripped of identifying features to reduce users’ concerns about Big Brother surveillance systems.

The value of information is beginning to have an increasing impact on user privacy (Langheinrich, 2002; Lessig, 1999). Advances in computers and communication technologies have substantially reduced the costs of collecting, processing and redistributing personal data, and it is relatively inexpensive to develop, maintain and transfer very large databases containing extensive amounts of individually identifiable and sensitive information (Robbin, 2001). This information is now a commodity valued by system developers, researchers, advertisers and most businesses, and is traded as such (Kenny & Borking, 2002). Gathering contextual information on the environment and users’ interactions with services can also provide system designers with the information to improve their services and better cater to users’ needs. User privacy is now an interaction between parties that have different preferences over information permeability (Jiang, Hong & Landay, 2002), and there is no guarantee that the user will be identified as the most important stakeholder.

This tension between privacy and information’s utility means that a balance between gathering useful information and maintaining the user’s privacy must be struck. Sensors can collect non-identifiable user information, services can be designed to be used anonymously, and access to and control over user data stored in an environment can be given to the user, for example privacy tags (Jiang & Landay, 2002). Anonymisation techniques can also be applied to user data to allow its use while maintaining user privacy (Canny, 2002). Intelligent environment designs must therefore acknowledge their potential harm to users’ privacy and seek to minimise this harm whilst providing valuable services that outweigh the potential risks involved.

Privacy can be broken down to examine what influences affect users’ interactions with an information system. Lessig (1999) categorises the four environmental regulatory forces on privacy as the Law, Market Forces, Social
Norms and the system’s Architecture. Each of these forces has an impact on the user's privacy and the other environmental forces. For example, laws are created in response to social norms and market realities, and society’s perceptions of what is possible and acceptable shift with the availability of new technologies; system architectures are created within these social and legal constraints. The design of a private and secure architecture must acknowledge the influences of the other three regulatory forces and allow them to impact on the exchange of information.

Users’ perceptions of these influences must also be allowed to be expressed in their privacy-based decision making processes. Adams (2000) identified the effect of the sensitivity of the data, the user’s perception of who may receive the information and what the data will be used for, on the user’s perception of the privacy of an information exchange. This process of analysing the risks versus the potential benefits of the information exchange is the same process that all people undergo when sharing sensitive information. Intelligent environment designs must support users’ ability to make this determination by ensuring they have access to all required information.

Lederer, Dey and Mankoff (2002) describe how users react to these influences by referring to the ‘preferred privacy level’ or ‘face’ that is adopted by users in a given situation. These authors combine the above contextual influences with the user’s perception of what information is being disclosed with generic contextual variables (e.g. activity, location and companions) (Lederer, Dey & Mankoff, 2002). These influences are based upon Lessig’s (1999) and Adams’ (2000) regulatory forces and users’ perceptions of privacy described above. This information must be provided as feedback before an information exchange, to allow users to effectively assess the risk of the exchange and to determine the appropriate persona they wish to use.

This shows the users’ context, and their perceptions of the architecture’s design and the information’s value affects the personal information, or the persona, a user wishes to share with the environment. Lederer, Mankoff and Dey (2003) further addressed the influence on the users’ context of information sharing. They examined the influence of the situation of the information request and the identity of the inquirer on the users’ information sharing preferences. They found that the inquirer, not the situation, had the bigger impact on what a user divulged in a given situation.

Users must therefore be able to control who they are sharing information with, and under what context this information sharing should occur. The management of contextual information within an intelligent environment has implications for users moving between multiple intelligent environments. For example, an employer should be able to access a user’s location while at work (the user’s location context), but should not have access to their location within a different intelligent environment outside of work hours.

Intelligent environment research and design should focus on technological feasibility and user-centred design (Abowd, GD & Mynatt, 2000). Privacy can be improved by anonymity and pseudo-anonymity, but this can reduce the effectiveness of certain systems (e.g. User adaptive systems). Trust and
reputation systems can provide users with the information to manage risks to their privacy, whilst identity management can limit the exposure of personal information to an intelligent environment. This section examines these and other concepts, and seeks to identify an effective balance of privacy protection and usability.

### 2.4.1 Privacy Regulation

Modern privacy legislation has been around since Warren and Brandeis (Warren & Brandeis 1890) moved to prevent the ‘unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers’ that was widely seen as a threat to privacy at the time. The first laws that expressly protected information privacy were passed in Europe with the Wes German Land of Hesse passing its Data Protection Act in 1970 (Clarke, 2000), around the same time as the Fair Information Practices (FIP) were gaining widespread attention.

In 1980 the Organisation for Economic Co-operation and Development (OECD) produced guidelines for the 'Protection of Privacy and Transborder Flows of Personal Data' (OECD 1980). These guidelines were developed to counter the concern that ‘disparities in national legislations could hamper the free flow of personal data across frontiers... [and] restrictions on these flows could cause serious disruption in important sectors of the economy’ (OECD 1980). This legislation is based upon the FIP (see above) and is more a codified requirement to promote the flow of information that any serious attempt at improving user privacy. The OECD guidelines describe a number of principles that provide recommendations on information storage and exchange, including the Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation and Accountability Principles (Clarke, 2000).

The European Union (EU) has more extensive privacy legislation that began with the European Convention on Human Rights and Fundamental Freedoms (ECHR) (1950) explicitly stating that everyone has a right to privacy in private and family life. The European Union further developed their privacy legislation by extending the 1980 Organisation for Economic Co-operation and Development (OECD) guidelines on the 'Protection of Privacy and Transborder Flows of Personal Data' (OECD 1980). Further limited legislation was passed throughout Europe and elsewhere until the United Nations adopted the Guidelines Concerning Computerized Personal Data Flows (UN, 1990).

Directive 95/46/EC (1995) states that users must have access to all information held about themselves, that data should only be collected with the individual’s explicit consent or with the authority of law, and that the data must be destroyed when it is no longer needed for the original purpose. Directive 2002/58/EC (2002) extends this to the telecommunications sector and explicitly mentions location-aware technology like that which is found in ubiquitous computing environments. The EU data protection directives also state that information transfers between countries must only take where the country receiving the information has equal or better privacy protections than that in the exporter’s country.
Later United States Supreme Court decisions suggested that the 9th (and to some extent the 3rd, 4th and 5th) Amendments to the United States Constitution provided personal privacy protection (Price, Adam & Nuseibeh, 2005, p. 233) but strong privacy protection is not explicitly stated or coded into US law. The US instead relies on a patchwork of privacy laws addressing particular privacy concerns like protecting information on financial (Gramm-Leach-Billey Act 1999) and health insurance sites (Health Insurance Portability and Accountability Act 1996) and safeguarding children online (Children’s Online Privacy Protection Act 1998); although some states do have stronger laws (e.g. California (Claburn 2005)).

Privacy protections demand a multi-tier approach, involving individuals, organisations, industry associations and governments, operating within a legislative framework (Clarke, 1999b). The New Zealand Privacy Act (passed in 1993 (Rose, 2006)) is an effective implementation of a set of comprehensive organisational, procedural and technical measures that exercise control over non-compliant organisations. The legislation seeks to encourage compliance (by creating economic and social incentives for ‘good citizenship’), and to discourage non-compliance (by creating social and economic disincentives, such as higher cost-profiles, and formal sanctions) (Clarke, 1999b).

Japan was one of the first countries to explicitly legislate privacy regulations for location-aware computing. This early adoption has led to improved business confidence in the market leading to a wider proliferation of ubiquitous computing services, and increased user confidence which lead to greater services utilisation (Price, Adam & Nuseibeh 2005, p. 236). Intelligent environments that automatically sense and identify users would be of questionable legal status in the EU and Japan.

There are over 20 national Data Protection and Privacy Commissioners, and some 20 in such countries as Canada, Germany, Switzerland and Australia (Clarke, 2000). Many of these agencies are seriously constrained in their work by under-resourcing, over extension of resources, insufficient legal authority, and their inability to level inadequate sanctions. They are also not consulted by governments (in the development of policy and in the drafting of new laws), have the advice they provide to governments ignored, are captured by organisations they are required to regulate, subject to direction by government (rather than reporting directly to Parliament), and are subject to resource reductions (Clarke, 2000). These constraints make the likelihood of these countries Data Protection and Privacy Commissioners effectively promoting privacy legislation to address the privacy problems, examined above in section 2.4, remote.

The differences in privacy legislation could cause problems for an intelligent environment architecture being rolled out across multiple countries. Users are also often ignorant of relevant legislation and have little faith in privacy policies, which makes the use of effective privacy system design and privacy defaults to secure users’ privacy critical (Berendt, Gunther & Spiekermann, 2005). This suggests that a minimum level of privacy, determined by users’ privacy perceptions and by the most restrictive privacy laws, should be
integrated into any intelligent environment’s architecture. An architecture that allows anonymous interaction and (where possible) service delivery is crucial in developing a widely adopted ubiquitous computing infrastructure that spans multiple countries, privacy regulations and perceptions of privacy in different cultural groups.

### 2.4.2 Privacy Design Strategies

Users interacting with an intelligent environment to obtain a service must (implicitly or explicitly) weigh up the benefits of the service received against the risks of providing personal information to the environment. Much research into ubiquitous computing systems suggests that if users do not perceive sufficient privacy safeguards on ubiquitous computing systems, then they are unlikely to use them (Kobsa, 2001; Lahlou, Langheinrich & Röcker, 2005; Langheinrich, 2001; Patrick & Kenny, 2003). This is despite the findings that many users are willing to trade privacy to receive something of value, whether actual or perceived (Berendt, Gunther & Spiekermann, 2005). This can be seen in the mass adoption of supermarket cards which collect extensive information on a user’s shopping habits in return for rewards or a slight discount, despite the potential for the abuse of this information (e.g. Vogel, J, 1998). Privacy in this case, then, could be framed as the management of users’ privacy expectations versus the value of the services.

It is essential to manage the flow of user information within ubiquitous computing environments to prevent the breaches of privacy that occur when information crosses personal borders of privacy (Marx, 2001b). Any use of personal information within these environments must restrict its flow across the natural, social, spatial and ephemeral borders of privacy (Langheinrich, 2002). Intelligent environments should restrict the flow of information outside of the physical location where it was provided, use it only for the purpose it was collected and delete it after a stated timeframe. Furthermore, services must be developed with sufficient interaction safeguards to prevent malicious users from conducting inference attacks on the service or environment’s databases. These principles should only be varied with explicit user consent or authority of law. These measures are fundamental if these systems are to respect individuals’ expectations of privacy in public spaces (Marx, 2001b). These concepts and solutions for controlling information flow are examined further in section 2.4.7.

An ongoing problem with user interactions within intelligent environments is the representation of information collected within the environment. Intelligent environments must enable people to be aware of how they are being sensed, without overloading them with information. The next step is to allow those being sensed or recorded to either stop this activity, or allow them to control the distribution and use of the information (Abowd, GD & Mynatt, 2000). The effective delivery of this information collection feedback is essential to allow users to determine impacts of an exchange to the user's privacy.

Patrick & Kenny (2003) describe a set of factors for effective privacy design in HCI environments such as intelligent environments: 1) Comprehension, 2) Consciousness, 3) Control and 4) Consent. These factors should be
Chapter Two: Background Literature

acknowledged when designing and implementing an intelligent environment to ensure users’ privacy and to promote the intelligent environment’s use. These principles are similar to the ‘Privacy Mirrors Framework’ (Nguyen & Mynatt, 2002) that requires ubiquitous computing systems to provide users with an interaction history, feedback to promote awareness and accountability, and allow the user to alter collections of their personal information. This awareness and accountability of actions and information exchanges allows users to make changes to their technical, social or physical environments to better integrate these socio-technical systems into their lives.

The concept of proportionality has been adapted from legal and data protection communities to allow the assessment of the usefulness of a system versus the burden it places on an individual or group’s privacy (Iachello & Abowd, 2005). The proportionality framework is used to 1) improve the system requirements gathering process, 2) provide the design process with grounding in legal practice and 3) expand the scope of analysis to technologies that do not necessarily afford intentional interaction (i.e. intelligent environments) (Iachello & Abowd, 2005).

The proportionality method is a useful method for evaluating the legitimacy, appropriateness and adequacy of a system with respect to user privacy (Iachello & Abowd, 2005). The adequacy of a solution is evaluated in a more tacit way, reflecting the fuzzy nature of privacy within these environments. The authors view privacy-enhancing design as risk management on information abuse, linking the cost of accessing personal information by an abuser, the perceived benefit deriving from abuse, and the cost sustained by the victim of such abuse’ (Iachello & Abowd, 2005). This fuzzy concept of privacy is also present in the information asymmetry work by Jiang et al. (2002) and reflects the adaptive social nature of privacy. Further privacy design guidelines and advice for ‘disappearing computing’, real-time collaboration and e-commerce systems are examined in the following sections.

2.4.2.1 European Disappearing Computing Privacy Design Guidelines

Ubiquitous Computing systems may take initiatives in data collection (Lahlou & Jegou, 2003), potentially collecting data beyond individuals’ awareness. This suggests that any developed design guidelines should focus on the specific issues of the data collection phase by such systems. Privacy enhancement is better obtained by actively constructing a system exactly tailored to specific goals than by trying to defend ex-post a poor design against misuse or attacks (Lahlou & Jegou, 2003).

The European Disappearing Computer Privacy Design Guidelines were developed by the European Community IST/Disappearing Computer Initiative, in the Ambient Agoras programme (IST-2000-25134). These design guidelines for privacy are aimed at system designers and stakeholders to allow more effective evaluation of the user and system requirements to provide privacy in disappearing or ubiquitous computing environments (Lahlou & Jegou, 2003). The nine design guidelines are: ‘think before doing’, ‘re-visit classic solutions’,
Chapter Two: Background Literature


The ‘think before doing’ guideline calls for the privacy implications to be evaluated with the stakeholders before the system is designed, to allow a non-biased evaluation of the privacy implications of the system. Developers should exercise responsibility by refusing to contribute to privacy damaging systems. Where possible, existing solutions that solve privacy concerns, potentially in other settings, should be considered and may be a useful starting point in the system’s development. Ubiquitous computing systems must be open in their objectives, uses of information and effects on the user.

The ‘avoid surprise’ guideline calls for more effective feedback on the consequences of interacting with the system. This is crucial in unobtrusive disappearing computing systems where information collection may be unclear. The ‘privacy razor’ calls for a default state in which the minimum amount of information required for a system is used, for example, identity is seldom necessary, and that data is not distributed without necessity. The list of requested information must be clear, and its exchange should be up to the user (Lahlou & Jegou, 2003). Feedback to the user should be effective, but should not overwhelm the user or make unrealistic calls for approval of data transfers. This invisibility versus adequate feedback is a classic design issue in intelligent environments, and is similar to the approximate information flow guidelines (among others).

The ‘third-party guarantee’ guideline suggests the use of third parties to improve the visibility of the information exchanges between systems and users, and to allow verification, validation, control and archiving of the information flow while minimising the information that needs to be collected by the system. Making privacy threatening operations expensive reduces the ability for mass breaches of privacy, and allows necessary breaches (e.g. emergency access to medical records) to be planned for. The final guidelines, ‘consider time’ and ‘good privacy is not enough’, ask the developers to consider the trade-offs between functionality, security and privacy (e.g. expiry dates on information) and to make these explicit to the systems’ users. Systems should also allow for change, and provide feedback and complaint mechanisms to allow for shifting social attitudes and the application of social forces to improve privacy within the system.

These guidelines provide clear guidance on the development of privacy aware ubiquitous computing systems. Information collection should be limited, user controlled and only used for specific purposes that provide value to the user. Above all, the purpose of these design goals is to orientate system design around the users’ interaction needs and to avoid unintentional (or otherwise) breaches in their users’ privacy. Any ubiquitous computing infrastructure that seeks to gain widespread acceptance must embrace these design goals and openly promote user privacy and information security.
2.4.2.2 User Privacy using Distributed Communication Systems

In order to consider how users will interact with intelligent environments, we need to consider how they react in similar settings where communication between users is possible. Instant Messenger systems allow not only contact between users, but also the exchange of contextual information about the user to be shared. This type of interaction functionality has also been suggested for use in intelligent environments, and an investigation into users’ perceptions of this technology may assist in the understanding of users’ privacy requirements for intelligent environments.

Patil and Kobsa (2004) conducted seven in-depth interviews with frequent users of Instant Messenger (IM) systems in order to investigate their privacy expectations and perceptions. The semi-structured interviews examined users’ routine use of IM in their daily lives and their expectations and behaviour regarding privacy. The authors identify that users shared three main privacy concerns:

- privacy from non-contacts,
- privacy regarding availability, and
- privacy regarding the content of Instant Messenger communications.

Privacy from non-contacts describes the desire for most people to be selective about to whom they allow access to their profiles and availability profiles (Patil & Kobsa, 2004). People on a contact list normally have a greatly lowered privacy barrier, and thus most users (with one young user being an exception) tended to be very careful about who was on their contact list. Subjects took great pains to make sure non-contacts could not see anything about them. These different types of privacy must be provided to users of the dissertation’s intelligent environment architecture.

Privacy regarding availability describes users’ desire to be free from interruption (Patil & Kobsa, 2004), by controlling their context information within the current group they have associated themselves with (such as work colleagues or friends outside of work hours). Users often reported using plausible deniability for unavailability, and this control of information is essential. This further suggests that users should be able to control all information about their current context and actions.

The privacy of content describes the need for users to keep their messages private, especially from persons mentioned in the communications (Patil & Kobsa, 2004). Most subjects expressed unease about their conversations being saved by their contacts, and all subjects reported switching to a more secure medium for conversations they deemed too private for Instant Messenger. A secure method of interacting with other users and intelligent environment services is essential to ensure users are able to maintain the privacy of their information flows. Patil and Kobsa (2004) suggest that the main drive behind these privacy concerns is the desire to control how others perceive the user, and intelligent environments should adopt these privacy requirements.
2.4.2.3 Privacy Behaviour in E-Commerce

The difficulty in investigating users’ behaviour and perceptions of privacy is the gap between what users state they do and what they actually do. This problem is exacerbated by the still experimental nature of ubiquitous computing systems. Users have yet to have access to a commercial intelligent environment that they interact with to obtain a valuable service beyond the situational awareness and tracking systems described in section 2.3.1. A useful tactic to address this problem is the evaluation of similar systems in which users can provide information to receive something of perceived value. This section, therefore, examines an investigation of users’ stated privacy preferences versus their actual behaviour when interacting with e-commerce systems.

Berendt, Gunther and Spiekermann (2005) analysed 171 questionnaires studying user perceptions of privacy and their experiences using an online shopping website. These questionnaires identify that users are concerned about their privacy and often adopt tactics to reduce risks to privacy while online. These include using false names, giving false information about their personal habits and avoiding potential privacy threatening websites. These concerns have led to the development of privacy enhancing technologies (PETs) such as P3P, based upon the idea that users study Internet privacy statements and then act in accordance with their privacy preferences. But this is often not the case.

The authors suggest that users often forget privacy preferences, particularly when the exchange is entertaining and the user perceives some benefit from the exchange (Berendt, Gunther & Spiekermann, 2005). In the study, users were interviewed about their use of an online shopping website that uses an anthropomorphic shopping bot to help them make decisions on which products to purchase. The questions allowed the researchers to profile the shoppers, and then consider the effects of their stated privacy preferences on their provisions of personal information. The research concludes that people seem to abandon privacy preferences when convenient, and suggests that privacy protection software (like P3P) may be more effective protection.

This research suggests that users will often give up private information when they can see some benefit from the exchange. While this may suggest an evaluation of the risks associated with providing the information against the reward, in many cases users gave away information about themselves without any compelling reason to do so (Berendt, Gunther & Spiekermann, 2005). Website privacy statements had little or no impact on most users’ behaviour, but statements that referred to EU Privacy Directives caused more people to provide their address. This is concerning, as it suggests that the more people believe in the jurisdiction, the less they control their personal behaviour (Berendt, Gunther & Spiekermann, 2005). This suggests that privacy statements should not be used to control user privacy, which implies that privacy management must be integrated into the intelligent environment architecture itself.
The lack of care shown by users in this study led to a call by the authors for more effective control to be placed in the software we use to interact with the Internet (Berendt, Gunther & Spiekermann, 2005). Current software (P3P) is limited to identifying when a website might breach the privacy concerns, but is unable to act on a per-service level. P3P also is not scalable to meet the privacy needs of more intelligent infrastructure in the future. Future architectures of this sort must control the flow of information and safeguard users’ privacy. Users shouldn’t be responsible for their own privacy; this should be secured at the electronic information exchange level.

The authors also call for more user control of PETs, the use of user pseudonyms and identity management, the use of intelligent agents to learn about the user’s privacy concerns, more private PET defaults and the use of third parties to manage privacy reputations for businesses and intervention in information exchanges by the PETs (or the intelligent agents) to highlight privacy concerns to users (Berendt, Gunther & Spiekermann, 2005). These suggestions are equally valid for exchanging information in a ubiquitous computing environment, and should be incorporated into any intelligent environment architecture design.

### 2.4.3 Privacy Enhancing Technologies

Privacy Enhancing Technologies (PETs) describe any technologies that are designed primarily to maintain or improve users’ privacy in a given situation. Privacy-Sympathetic Technologies (PSTs) is a term invented to convey the role of the technologies in ensuring user privacy whilst at the same time providing accountability that is often needed for repudiation or complaint resolution (Clarke, 1999a). PSTs protect the user’s identity under normal conditions, but this veil of secrecy can be lifted when compelled to do so by the issuing organisation or legal mandate.

PETs within intelligent environments can be aimed at many different points in the architecture in which user privacy could be breached. Identity management software could be used to maintain the desired level of anonymity when accessing services. Biometric applications like fingerprint scanners or voice recognition software can secure mobile devices and prevent identity theft, or ‘iJacking’. Single use and reloadable credit cards can protect users from credit card fraud and prevent the compilation of extensive user purchasing histories that have already been shown to be a privacy risk (Vogel, J, 1998).

Berendt, Gunther et al. (2005) conducted extensive research into users’ stated privacy preferences versus their actual behaviour, and they have identified some valuable, and worrying, findings on users’ interactions with existing PETs and e-commerce shopping websites. This work identified that users will often give up information when they perceived value in exchange. The Tesco (or Safeway) shopping reward cards allow the tracking of all users’ purchases, and provide each business with enormous amounts of information on shopping habits and direct marketing opportunities, in exchange for a small/negligible discount or rebate on their purchases.
Users of the e-commerce shopping websites in the study also demonstrated that the privacy statements provided by the sites had no impact on most users’ behaviour (Berendt, Gunther & Spiekermann, 2005), even if the users claimed otherwise. Further findings found that mentioning existing data protection legislation led to users sharing more information, suggesting that the more people believe in the effectiveness of existing jurisdiction, the less they control their personal behaviour. These findings suggest that users should not be solely responsible for their privacy, nor should it be left solely to government legislation.

The Liberty Alliance project developed a web services framework that provides identity services to users interacting with different web services. The framework provides standardised communication syntax and semantics to validate aspects of the user’s identity (Liberty Alliance, 2002), and consists of service discovery, identity mapping, interaction and authentication services. To improve usability, the Liberty Alliance framework uses a single sign-on service that allows the user access to all their identity services with just one password. The relationships with multiple identity providers are managed using their mobile device.

The Shibboleth architecture extends the SAML 1.1 single sign-on and attribute exchange mechanisms by specifying service-provider-first SSO profiles and enhanced features for user privacy. The functional components of a conforming Shibboleth implementation include an identity provider, a service provider, an optional “Where are you from?” (WAYF) service, and various interacting subcomponents (Shibboleth, 2005). The identity provider provides an authentication authority, a single sign-on service, an attribute authority (that can issue attribute assertions) and an artefact resolution service (that stores the user’s identity information). The identity provider can therefore provide (in a secure manner) identity assertions about a user that has a pre-existing relationship with the provider.

The Shibboleth service provider manages secured resources, which could range from access control on computing resources (e.g. printing) to the delivery of a service. The service provider integrates with the single sign-on service (for secure communication) and the user’s identity provider to validate user’s rights to access the resource. Shibboleth does not prescribe the types of identity attributes that are required for identity assertions, nor does it define the services that can or cannot be supported in the architecture. The SAML definitions for asserting authentications and user attributes (e.g. identity authentication assertions) in Shibboleth are described in detail in the architecture’s technical overview (Shibboleth, 2005, pp. 7-12).

OpenID is a community driven, open specification for communicating identity information securely between parties similar to the Liberty Alliance and

---

3 The Liberty Alliance Project framework, design specifications and all related materials were later contributed to the Kantara Initiative (http://kantarainitiative.org/), and the development of an effective web-based identity interaction framework continues.
Shibboleth frameworks. OpenID supports URLs and XRIs as user identifiers, uses Yadis XDS documents for identity service discovery, and supports both public and private identifiers (Recordon & Reed, 2006). OpenID uses address-based (unique digital address) or card-based (digital tokens) identifiers to prove users identity. The user provides the identifier to the requesting entity, and the identity provider validates the identifier and sends the information directly to the requestor in SAML or similar forms.

A U-Prove token is a cryptographically protected container of attribute information that can be distributed by any issuer (e.g. user or identity provider). Each U-Prove token corresponds to a unique private key that its ‘Prover’ generates in the issuance protocol (Brands & Paquin, 2010). When using a U-Prove token, the Prover applies the token’s private key to the message to create a presentation proof (non-repudiation of the message). This provides the receiver with proof-of-possession of the private key, and provides the digital signature of the Prover on the message. The presentation of the token to another party does not reveal its private key, and the token cannot be stolen through eavesdropping or phishing and prevents replay attacks by legitimate verifiers. The U-Prove token can be used to sign as many messages as required.

U-Prove tokens can also be configured at issuance time to include as much information as required. This allows the tokens to be used to provide identity, service preferences or any other information that is relevant to the user’s required activities. The strength of the cryptographic protection for the tokens is dependent upon the quality and secrecy random number generated for use in the encryption process, and the key length used to encrypt the token and digitally sign the accompanying message (Brands & Paquin, 2010). The protocol used for creating, presenting and verifying the U-Prove tokens is described in (Brands & Paquin, 2010).

Tor is a circuit-based, low latency anonymous communication service. It provides a communication network that allows anonymous interaction, prevents the local system from gathering extraneous information about the user (e.g. Tor prevents the destination of a user’s identity provider from being collected through perfect forwarding secrecy) and provides ‘Trusted’ nodes that act as directory services. Tor also implements a number of network management techniques to improve the anonymity of user interactions and communications. Mix Zones (Ref) can further be used to obfuscate a user’s interactions within the Tor network by changing communication identifiers in areas of high traffic (see section 2.4.7).

A noted issue in the Tor network is the ability for users to anonymously engage in Denial of Service attacks or to abuse the network resources for spamming or other attacks. To prevent this abuse it is suggested that the network include initial communication handshake requirements that are computationally expensive to conduct (and would therefore make denial of service or spamming operations less efficient). Tor also uses a small group of trusted routers to track changes to the Tor network topography and makes trust determinations on individual directory services.
The Platform of Privacy Preferences (P3P) protocol is was developed by the World Wide Web Consortium (W3C) to allow users to provide some guidance on their expected privacy and interaction preferences whilst interacting with services on the Internet. The protocol explicitly recognises the need to support multiple personae per web-user (Clarke, 1998c), allowing users to interact with the web services using a range of different privacy and interaction requirements. Personae allowed web-users to be able to create different views of themselves, and select which of these persona they wished to interact with at any given time based upon their current interaction needs. It was established to improve trust between services and users on the Internet, and to provide assurances of data collection and reuse to allow users to make determinations about the impact of a service on their privacy.

The elements of the P3P are the user’s privacy preferences (expressed as rules for exchange of information), web-site data use and disclosure practices, the P3P protocol (which governs the interaction and exchange of information) and the P3P-compliance system (that governs how the web-browser, server and proxies act) (Cranor, L.F., Langheinrich, Marchiori, Presler-Marshall and Reagle, 2002). Upon connecting to a P3P compliant web-site, the user’s privacy preferences are compared to the site’s stated privacy practices that describe what information is collected and how it is used. If there is a mismatch, the user is informed of the potential privacy hazards and they are given a choice of not connecting to the web site (or taking other action).

P3P does not offer a complete privacy solution. Clarke (1998b) describes a number of problems with the effectiveness of the privacy protection offered. Many of the OECD Principles for effective privacy design are overlooked, including:

- practices relating to data collection;
- data storage and retention;
- data quality;
- controls, against the data purpose, over actual use or disclosure;
- subject access to data held by the website operator; and
- accountability, and sanctions for non-compliance.

Key questions about P3P are:

- is the privacy protection afforded a significant enough contribution?
- Is the fair information practices paradigm, on which the P3P vocabulary rests, rich enough to reflect legal and culture diversity?

Environmental factors are, however, even more important determinants of its success and failure. Key questions are:

- will web-users consider web-site providers’ statements to be sufficiently credible that they will express their privacy preferences in P3P?
- will web-site providers express their privacy statements?
- crucially, will web-site providers comply with their privacy statements?
It is clear that the privacy protections offered by P3P do not go far enough. The credibility of the system rests on the belief that a foreign system will act as described. Similar concerns arise when interacting with unknown service providers in ubiquitous computing environments. P3P does not reach its original goals for protecting user’s privacy. In its current form it is more of a ‘privacy policy declaration’ standard than a privacy policy enforcement protocol, but the intention to allow users control of their privacy and to warn them of potential consequences to their privacy from a particular service interaction has merit.

2.4.4 Identity Management

Identification is a process whereby a real-world entity is recognised and its identity established (Clarke, 1999a). At this point it is useful to acknowledge the difference between an identity and an entity (described as (Id)entity when either term could apply). An entity is a real world thing (e.g. a person, object, animal, organisation, etc.), while an identity is an abstract concept that describes a representation (or label) of an entity. An entity does not necessarily have a single identity, but may have multiple identities each reflecting a different representation or role the entity plays (e.g. with their families, organisations, the government, etc.) . This ‘many identities to one entity’ relationship is important when considering the interaction users have with intelligent environments.

Identities are identified via an identifier. An identifier is a characteristic of the identity that can be used to distinguish the identity from others in the same category (Clarke, 2009). Examples of identifiers include a person’s name, a social security number, or an alias that is associated with the identity. An identifier is associated with an identity, and not with the underlying entity. Similarly, an entifier is an attribute that can be used to distinguish an Entity from others in the same category (Clarke, 2009). Examples of entifiers include a biometric signature (for a person) or a serial number (for an artefact). The process of confirming an entity is called entification.

The (id)entification process involves the assertion of an (id)entifier, the authentication of that assertion, and the authentication of that identity. An assertion is a statement of a fact (or an (id)entity attribute, data quality, location or agency) made by a particular entity. Identity assertions are therefore statements that assert that an identifier is being appropriately used, or that the identity in question is who or what it purports or is inferred to be. An entity assertion similarly states that an entifier is being used correctly, or that the entity is who they (or it) purports or is inferred to be (Clarke, 2009).

Authentication is the process that establishes a level of confidence in an assertion (Clarke, 2009). Authentication is performed by cross checking an assertion with one or more authenticators. The assertion in this case may be a written signature or the characteristics of an object provided to the authenticator. Credentials are general terms for an authenticator that has a physical or digital existence. An example of a credential is a token or
document that demonstrates the entity’s identity or agency for a particular organisation. **(Id)entity Authentication** is the process whereby the required level of confidence is achieved for a given (id)entity assertion. (Id)entity authentication is quite distinct from (id)entification, which is where data is associated with a particular identity by acquiring an (id)entifier for it (Clarke, 2009).

Identity knowledge describes the level of knowledge about a given user’s identity. Identity knowledge has multiple components, and there are degrees of identifiability. Marx identified seven broad types of identity knowledge (Marx, 2001a). These are 1) legal name, 2) locatability, 3) pseudonyms that can be linked to legal name and/or locatability – literally a form of pseudo-anonymity, 4) pseudonyms that cannot be linked to other forms of identity knowledge – the equivalent of ‘real’ anonymity (except that the name chosen may hint at some aspects of ‘real’ identity), 5) pattern knowledge, 6) social categorisation and 7) symbols of eligibility/non-eligibility. The ‘legal name’ identifier technically has no real world equivalent, but is comparable to the term ‘entity’ used above. Social categorisation could be any identifier given to a person by society (organisations, government departments, etc.). Symbols of eligibility/non-eligibility are not a level of identity, but reflect the ability to identify to another organisation or party that the holder is one of the others.

The authentication of an identity assertion provides a system (or entity, etc.) with a level of confidence about the identity of the interacting party. The level of confidence ranges from no confidence (unauthenticated) to high confidence. Or said another way, the identity could be said to be strongly, moderately or weakly authenticated, or unauthenticated (Clarke, 2009). The more identity providers that can be utilised to authenticate a given identity, the stronger the confidence in the identity will be. The architecture developed in this dissertation must provide the user with a multitude of identity providers with which to authentication their identity.

In this case the authentication of pseudonyms or ‘legal names’ is the same. Authentication of a persistent nym (or pseudonym) can be an effective means of establishing confidence that a series of communications are with the same person, even though the identity of the person is not reliably known (Clarke, 1999a). This authentication is similar to the authentication of a user’s service delivery pseudonym, and will allow the service provider to verify that the service user is the same person that previously used this account. The concepts of anonymity and pseudonymity are investigated further in section 2.4.5.

A digital persona is a digital reflection of an aspect of a user’s real world identity. This could include the user’s complete identity, or a subset of their identity that is used for a specific purpose. An individual is likely to have multiple personae at any given time, reflecting different aspects of their personal or digital identity. Digital personae include the ‘projected persona’ which the user creates to represent themselves, or the ‘imposed persona’ that is created by others (Clarke, 1994). Digital personae can be created through matching of information on the user from multiple sources, via a common identifier, by correlating data using multiple identifiers, and through multi-
attribute matching (Clarke, 1994). The meaning of a given persona is entirely
dependent upon its receiver, based upon their own processing rules.

There are many difficulties in achieving effective multi-attributive matching of
personae. Problems arise from the quality of the data, its source and the
context of its use. Further trouble will occur when intelligent environment and
their services attempt to combine data provided freely by users that have a
vested interest in obfuscating their personal data to improve their privacy.
These defensive privacy strategies may play a large part in the use of
ubiquitous computer services and the ability to secure user's privacy in these
environments. This type of protection could have negative consequences for
the user however, as providing false information could inadvertently match
the user to other personae or provide false positives that draw the attention
of law enforcement or service regulation authorities. Providing false
information may also bring about less important but more immediate
problems as services, advertising and contextual help may be personalised in
a manner to make it less relevant for the user. This could be addressed with
user practice as they learn what service information is important and what is
not.

Clarke further deconstructs personae into either active or passive personae
(Clarke, 1994). Passive personae are statements of information that describe
the user’s identity, characteristics or preferences. These personae can be
reductionist descriptions of a small aspect of the user’s identity, or could
theoretically describe every aspect of a user’s identity. Passive personae are
the most common type of personae, and users will normally have multiple
personae that allow them to conditionally represent aspects of their identity.
Active personae describe ‘agents’ that interact with the Internet or specific
systems on behalf of the user according to predefined behaviour or to achieve
a specific set of goals. The use of intelligent agents (or active personae) is
outside the scope of this dissertation, but is explored as ‘Future Research’
(see section 8.3.4).

Identity Management has also been described as system that enables each
user to express and to enforce his or her privacy and security needs in IT
systems depending on the situation the user is in (Jendricke, Kreutzer &
Zugenmaier, 2002). That is, it allows users to determine what information
about themselves may be shared with a given system, and therefore allows
the user to control risks to their privacy and security. This definition of
Identity Management is counter to the traditional definition of a set of
processes that enable the authentication of assertions of identity. Identity
Management Systems enable organisations that support user accounts to
authenticate assertions of identity by people seeking to use those accounts,
and perform ancillary functions such as pre-authentication, authorisation,
single sign-on, Identity repository management, synchronisation
management, user self-registration, user self-service capabilities, and audit.

Identity management has become increasingly important because users have
developed the need to represent difference facets of their identity to different
sources, in both the real and digital world. This is especially important for
ubiquitous computing environments, in which the user can interact with a
Chapter Two: Background Literature

wide range of environments in potentially rapidly changing contextual circumstances. The Jendricke et al. (2002) definition describes a situation where users have much more control over their plurality of identities compared to the more traditional (one user to one identity persona) relationship that dominates existing identity management systems (e.g. Liberty Alliance or the WS-Federation) (Koch & Moslein, 2005). This dissertation accepts both definitions are valuable, and while the ability to perform identity authentication in intelligent environments is important, users must also be able to manage represent themselves as they wish based upon their current needs.

Ubiquitous computing systems are unique in their potential to cover all of the physical environments in our everyday lives. Users are wary of these systems because often they do not provide the same level of anonymity or interaction possibilities as users enjoy with existing (traditional) physical services. To maintain user confidence and privacy, intelligent environments must allow users to represent aspects of their multi-faceted identity to systems as they choose to. This reflects the capability that they have to use multiple identities in the real world. Users must be able to prove their identity, act anonymously and maintain repeatable, personalised relationships with service providers. Providing users with the same tacit and explicit feedback enjoyed when interacting with an existing service is technologically a difficult task, but there is increasing evidence that feedback on the information exchange, for example the information’s receiver or the users’ context, is essential to maintaining user privacy (Adams, 2000; Jendricke, Kreutzer & Zugenmaier, 2002; Jiang, Hong & Landay, 2002).

Identity management is normally achieved (in the real world) through the use of identifying documentation issued by a central, trusted third party. Traditional brokers of identity include not only governments and financial institutions, but in addition other institutions that provide identity cards and store information on an individual, for example businesses or educational institutions. Koch (2002) describes ‘Infomediaries’ as client-side user profile storage structures that allow users to manage user information and can provide this information to third-party services. This personae storage does have the problem of portability between users’ computers, so users might require remotely stored user personae when interacting with intelligent environments using multiple handheld computers.

The digital revolution has provided additional methods of authenticating user’s identity assertions. The Liberty Alliance framework (http://www.projectliberty.org) and Microsoft’s U-Prove (Brands & Paquin, 2010) system provide centralised identity management that can be queried by third parties. This is a traditional view of identity, with the organisations managing the user’s identity from a single identity provider. Shibboleth (Shibboleth, 2005) and the OpenID (Recordon & Reed, 2006) architecture offer similar identity services, but is developed to provide a decentralised approach to identity authentication with the user’s being able to use multiple authentication entities to assert their identity. Other smaller identity projects focus on financial transactions (Yodlee http://www.yodlee.com/) and on
providing a federated approach that allows for the use of different identity services operated by different providers (XRI/XDI digital identity infrastructure (http://www.xdi.org/)).

The Liberty Alliance is a centralised identity management service that has evolved to allow interoperability between current identity management providers (e.g. AOL, VISA, etc.). The goal for the Liberty Alliance is to make it easy for services that are storing users’ profile information to exchange the information to each other (Liberty Alliance, 2002). But these centralised approaches do not allow users control over their identity profiles, and do not handle the complex user attributes needed to model relationships or interests (Koch, 2002). Other concerns with centralised identity management arise when collected information is used for additional purposes, as seen in the widespread rejection of Microsoft’s Passport (Bishop, 2004).

OpenID (http://www.OpenID.net/) is a free, secure and decentralised third-party identity structure that allows users to verify their identity to numerous websites with one login. Users of OpenID register an account on their website and, if they wish, populate their account with personal information. This account is then used to store site logins and passwords to allow the user to use this one account to sign in to all websites that support the OpenID system. These identity accounts would require users to prove their identity to the provider when signing up. A useful aspect of the OpenID service is that it records all verifications of the user’s OpenID account, allowing them to see their activity and providing a method of refuting false interaction claims. This would be useful for a ubiquitous computing environment. These architectures are described in more detail in section 2.4.3, while the identity assertion languages utilised by these services (e.g. SAML) are described in section 2.3.4.

Identity management and central user profile repositories might help a) to motivate users to make user profile information available (because they have control and awareness about who is using it) (Koch & Moslein, 2005) and b) services to provide effective personalisation without cold-start problems (Koch, 2002). These two effects could help boost the use of personalisation services. Technically, the most important challenges are a) how to specify (and enforce) access rights (especially including usability and user interface issues) and b) how to represent user profile data to make it usable by different services. The Personis (Kay, Kummerfeld & Lauder, 2002) and Personislite (Carmichael, Kay & Kummerfeld, 2005) modelling languages are XML-based notation standards for the creation, storage, management and exchange of user profile information. These modelling languages were examined in section 2.3.4.

The privacy principles for Identity Management can be derived from the requirements for multilateral security. These requirements are: Confidentiality (of message contents, anonymity and pseudo-anonymity and protection of location information), Integrity, Availability, Accountability, Notice or Feedback (of information collection for information management) and Data Collection (Data Minimisation, Personal Control and Non-Repudiation) (Koch,
2002). An effective Identity Manager fulfils all principles that do not rely on third parties, but much of these structures can also be integrated into the wider ubiquitous computing architecture.

2.4.5 Anonymity and Pseudonymity

Interaction with an intelligent environment's services can be identified, pseudonymous or anonymous. An identified record or transaction is one that can be associated with a particular person. An anonymous record or transaction is one whose data cannot be associated with a particular individual, either from the data itself, or by combining the transaction with other data (Clarke, 1999a). Anonymity is essential for maintaining users’ privacy whilst interacting with ubiquitous computing environments. This definition is especially apt in intelligent environments, where users’ past interactions can be compiled and lead to the construction of fairly comprehensive user profiles.

Pseudonymity enables actors in a system to reflect the various roles that people play in the real world (Clarke, 1999a). This enables people to interact with systems (or services) anonymously, in their capacity as a representative of an organisation or as their private selves. To be effective, pseudonymous mechanisms must involve legal, organisational and technical protections such that the link to the user can only be made under certain circumstances (Clarke, 1999a). Pseudonyms can be used to protect individuals in instances were using their real identity might cause undue embarrassment or physical harm. This interaction capability is essential in allowing normal real world interactions and in promoting the use of intelligent environments (by reducing the perceived risks to a user’s privacy).

Maintaining users’ privacy and the protection of user information can be accomplished through the anonymisation and encryption of user information (Kobsa & Schreck, 2003). Pseudonyms can also be used to ensure the integrity of users’ privacy. A pseudonymous record or transaction is one that cannot, in the normal course of events, be associated with a particular individual (Clarke, 1999a). However, the longer a pseudonym is used, the more likely it will be linkable back to its user. Therefore the use of multiple pseudonyms increases users’ environmental and content-based anonymity.

Location privacy can be defined as the ability to prevent other parties from learning a user’s current or past location (Beresford & Stajano, 2003). As systems become more effective at precisely locating a user, more thought needs to be put into the collection and use of this information if user privacy is to be guaranteed. Methods of providing (or improving) user anonymity involve disguising users’ hardware when interacting with ubiquitous computing environments (Gruteser & Grunwald, 2005) and the disguising of a user’s identity by switching pseudo-anonymous locators whilst within areas of high traffic (Beresford & Stajano, 2003). These are examined in section 2.4.7.2.

Anonymisation of user data and actions can reduce the effectiveness of systems that provide services to users based upon past and predicted
Chapter Two: Background Literature

behaviour. Developers and users must weigh up the benefits and risks associated with user anonymity and user-adaptive systems, for example criminal behaviour or increased usage. Anonymising user data is also a method for relieving the market pressure to use this increasingly valuable information source. Most privacy research suggests that anonymisation is a way of including user data, as long as there can be no way to link individual data to a user through advanced number crunching and data mining techniques (Canny, 2002).

The potential benefits of employing user anonymity and its popularity with users ensure its implementation (Kobsa & Schreck, 2003). Where possible, users should be allowed to remain anonymous in intelligent environments, and verifying identities should remain outside the control of an intelligent environment to reduce their access to user information. This research investigates the inherent tension of maintaining user privacy by using anonymity and pseudonyms, and the need to provide effective personalisation to overcome the invisibility problem associated with ubiquitous computing services.

2.4.5.1 Secure Pseudonymous Identity Management

A system has been developed to allow users to provide verified identity pseudonyms to a service provider without requiring the user to provide all their information (Hitchens, Kay & Kummerfeld, 2004). This ability greatly improves users’ privacy by providing a method of sharing only a subset of the user’s identity in a way that gives the receiver confidence that the partial identity as presented by the user is accurate. This system is comprised of two parts: a mechanism that supports users defining authenticated personae that can be pseudonyms; and mechanisms for users to share such personae with the service providers (Hitchens, Kay & Kummerfeld, 2004). This provides a secure, structured method for exchanging signed information with an intelligent environment using third-party certified templates.

Users use subsets of user models (called personae) to communicate information with another party. But in order for this information to be accepted and generally understood in an efficient manner, there must be a common repository of shared vocabulary available to both parties. This vocabulary is defined using templates built in a common modelling language, like XML, SAML or Personis (Kay, Kummerfeld & Lauder, 2002). The personae are digitally signed by a signatory when created, and this signature or authentication is used by the reviewer of a given persona to determine what trust is to be placed in it (Hitchens, Kay & Kummerfeld, 2004).

This system uses a preloaded mass of templates to satisfy users’ information distribution needs. Each persona is authenticated and signed and can be accepted by third parties. Additional unauthorised personae maybe made from these, and this could impact on the trust evaluation that takes place when information is exchanged. In this environment, there would be far more users than authorising entities, so they would be more visible, allowing intelligent environments to monitor their perceived trustworthiness (Hitchens, Kay & Kummerfeld, 2004). This use of a third party to confirm user
information is similar to the way people build trust, and can allow users to enjoy the same levels of anonymity experienced in the physical world.

This system describes a structured way in which users can share information with third parties in a way that it can be trusted as accurate without revealing private information. A user’s personal device would most likely have many such templates, and would select the most appropriate one for what they are trying to accomplish (or the one that best matches the service required). This would allow users to interact with intelligent environments in a private and anonymous manner, even when user information is required to personalise a service. This ability would allow users to obtain a number of signed personae from the authorising entity, which they could use across multiple environments, reducing the chance of being tracked by the environments and therefore further reducing risks to their privacy.

2.4.6 Trust and Reputation

Trust is a complex interaction between two parties that has numerous definitions. Trust can be described as the firm reliance on the integrity, ability, or character of a person or thing\(^4\). A common element of the usage of ‘trust’ is the expectation or belief that a particular entity will act as expected in a given situation (Cahill, Gray, Seigneur, Jensen, Chen, Shand, Dimmock, Twigg, Bacon, English, Wagealla, Terzis, Nixon, Serugendo, Bryce, Carbone, Krukow and Nielsen, 2003; Camp, 2000; Deutsch, 1958) and, conversely, the sense of unpleasant consequences that arise when trust is broken or wrongly assigned (Deutsch, 1958). Trust is therefore a two-way activity, where the act of assigning trust to something implies a responsibility for it to act in an expected manner.

The open nature of the protocols underwriting the Internet leads to the expectation (trust) that components will act as expected (Camp, 2000). This includes the confidence that a router will forward a packet to its destination and that the destination system (software, user, etc.) will be able to use the information as expected. Camp (2000) describes this trust network as similar to a social network, and identifies that the inherent ability to instantly route around points of failure as integral to trust across the Internet. This ability provides the Internet with a robustness that engenders trust and allows services to be provided regardless of the user's physical location. This trust is not automatically conferred upon services delivered via the Internet however, just in the delivery technologies themselves.

Trust is largely an invisible and implicit construct in our society (Cahill et al., 2003). This makes it difficult to quantify, and is a subjective notion that every individual must decide whether to trust based upon the available evidence (although this evaluation may be delegated to an authoritative source). The nature of trust means that it is dynamic and context-dependent, and trust evaluations will vary between users, circumstances and environments. Deutsch (1958) found that methods of mitigating outcomes or punishing the

\(^4\) http://www.thefreedictionary.com/Trust
trust breaker, the ability to know what the other person will do, and the power to influence the other party's outcome from the exchange all impact on the perceived trustworthiness of an exchange.

Humans use trust as a method to reason about and mitigate risks to their privacy, and they assign privileges accordingly (English, Nixon, Terzis, McGettrick and Lowe, 2002). For an interconnected system of potentially untrusted system components, like an intelligent environment, to be useful, there must be a method of dynamically determining trust and associating that trust with the information provided by the entity. Trust is evaluated by users using personal observations of previous interactions, the entity's reputation and recommendations of partly trusted third parties (Cahill et al., 2003; English et al., 2002). Trust evaluations can also be delegated wholesale to another entity (and potentially evaluated based upon the user’s trust of the third party).

User preferences for information sharing are based upon the known attributes of the inquirer, be it an intelligent environment or another user. Trust and reputation have been identified as useful influences on user preferences in the absence of other determining information (Goecks & Mynatt, 2002). The ability of two entities to communicate before an interaction greatly increases the trust between them, particularly if they are able to communicate a shared sense of values or expectations for the exchange (Deutsch, 1958). Intelligent environment designs must identify the impacts of the environment upon the users’ privacy, the effect upon users’ trust of the intelligent environments and consequently the intelligent environment’s reputation. The impact of each of these influences on users’ trust is examined in the user studies in chapter four.

The Personal Reputation System (PRS) uses a weighted evaluation of feedback based upon trust levels associated with the source (Goecks & Mynatt, 2002). These trust evaluations include self-determined trust levels and the trust opinions of people associated with the system (e.g. the trust opinions of a user’s friends). Trust evaluations were also used to determine the reputation of other users (Goecks & Mynatt, 2002). This may be a method of overcoming problems with user privacy preferences. Default settings of high privacy can exclude new users within an intelligent environment (much like only accepting emails from friends to reduce spam). The necessity for users to explicitly invite individual users to join in information sharing could cripple the benefits of a system’s scalability and mobility.

Trust and reputation systems are common in non-ubiquitous computing environments. Pretty Good Privacy (PGP) is a method of using encryption to create a web or chain of trusted parties between two points (Zimmermann, 1995a). This allows the current party to leverage the trust that already exists between other entities, for example, allowing the user to prove through the chain that a public key actually belongs to the person they are claiming to be (see section 2.5.3.1). Less secure systems can use user voting to reflect the approximate trustworthiness of an entity (user, seller, system etc.).
Trust and reputation systems are widely used on the Internet, a largely anonymous network where determining the trustworthiness of another party can be difficult. Ebay (http://www.ebay.com/) users can leave feedback on the trustworthiness of other buyers and sellers with whom they have done business. Slashdot (http://www.slashdot.org/) uses a similar reputation method to moderate the prominence of a user’s comments in their forums. These reputation systems are often used in large online communities where a user may frequently interact with users with whom they have had no prior contact, and give the user more information with which to make a judgement about the character of the third party.

The nature of ubiquitous computing environments makes the use of trust and reputation systems difficult. Intelligent environment interaction is often anonymous, and users often want to remain anonymous right up until they need to provide their identity to access a particular service. Users are unlikely to engage fellow users in activities that require trust, for example M-commerce. The most likely point of interaction with trust systems within intelligent environments is when users interact with their services. Trust or reputation rating systems would, however, allow users to verify the trustworthiness of services provided by the intelligent environment.

Users could record positive or negative feedback on a service provider that could be added to the progressive score shown to each user before they access a service, given their prevalence outside of ubiquitous computing environments and the existing research on their development within ubiquitous computing environments (e.g. Cahill et al., 2003; English et al., 2002). The dissertation is focused more on the appropriateness of their integration into the greater intelligent environment infrastructure than on the actual system used to collect and rate an entity's trustworthiness or reputation.

### 2.4.7 Management of Information Flow

The design of an intelligent environment must clearly define the flow of information between environmental entities. Where possible the control of information should reside with the information’s owner, and the system should provide appropriate feedback on information collection activities (Nguyen & Mynatt, 2002). The authors refer to the ‘Privacy Mirrors’ framework, in which users maintain an awareness of the information exchanged with the environment and its impact on their privacy. This feedback is necessary to reduce the invisibility of information flowing within intelligent environments, and to provide users with adequate information with which to judge any risks to their privacy. The types of information users require to assist in this evaluation are investigated through various user studies in chapter four.

Asymmetry of information describes situations in which some actors (in a given market or situation) hold private information that is relevant to everyone. An example of this would be the case of a used car dealer that knows the mechanical problems of a car (that the buyer is unaware of) when negotiating a sale price. In this case the buyer is at a significant disadvantage
before the negotiation. In an intelligent environment, a user might be in a similar position if they did not know about a particular information reuse policy of an service provider. This lack of information would make the ability to make an informed decision on the impact of an interaction to the user’s privacy impossible.

The existence of such asymmetric information has a significant negative effect on economic, social and legislative dealings (Jiang, Hong & Landay, 2002). The presence of asymmetric information between data owners and data users has significant effects on the first three of Lessig’s (1999) four regulatory forces on privacy (Markets, Social Norms and Legislation) (Jiang, Hong & Landay, 2002). The presence of asymmetric information is counterproductive to both the user privacy and to the efficient exploitation of the benefits of intelligent environments.

The design of an intelligent environment should manage information flows to minimise the asymmetry between the data owners on one side, and data collectors and data users on the other side (Jiang, Hong & Landay, 2002). Information asymmetry in an intelligent environment can be minimised by:

- decreasing the flow of information from data owners to data collectors and users, and
- increasing the flow of information from data collectors and data users back to data owners.

Users use personae in intelligent environments to achieve exactly this. A persona allows the user to provide a limited set of information to the environment. This decreases the extraneous information provided with an information request, and provides an easy-to-use method of interacting with increasingly sparse digital personae. The ‘Privacy Mirrors’ framework and the European Disappearing Computing Privacy Design Guidelines are examples of the type of information that should feedback from the data collectors and data users to the data owner.

Furthermore, control of the representational accuracy of information flows can have a significant impact on user privacy. For example, reporting a user’s location as an exact address would have vastly different implications than simply reporting their town or city (see location privacy below). By varying the resolution, we allow users to achieve intentional ambiguity, thus allowing them plausible deniability on their location. The effectiveness of this strategy will vary by the type of information provided and the size of the dataset being searched (if relevant). Price, Adam and Nuseibeh (2005) describe this as adding ‘noise’ to data to hide or disguise a user’s location or identity. This method of ‘social lying’ is necessary if we are to recreate the privacy users enjoy in the real world.

The ultimate goal of the principle of minimum asymmetry is not to provide a purely technological solution to privacy, but to make it easier for market, social and legal forces (Lessig, 1999) to be applied to address legitimate privacy concerns (Jiang, Hong & Landay, 2002). This principle ensures that more information is retained by the user, and less information is collected by the intelligent environment. This control of information collection and access
becomes particularly important when considering a user’s interactions with multiple intelligent environments, and the advanced data-mining capabilities that can be used to reveal information about the user.

Borrowing further from the legal community, other authors have suggested that the principle of proportionality should also be applied to information shared within intelligent environments. The principle of proportionality states that any application, system, tool or process should balance its utility with the rights to privacy (personal, informational, etc.) of the involved individuals (Iachello & Abowd, 2005). In practice, this principle is evaluated by judging an application’s legitimacy, its usefulness, its appropriateness, if it is built with the proper technology and its adequacy, or if the application is built properly.

This principle is similar to the European disappearing computing privacy design guidelines (Lahlou & Jegou, 2003) in its call to justify a system’s purpose, openness and impact on user privacy. This approach attempts to prevent systems from preying on normal user behaviour of choosing to interact with a system for a (potentially insignificant) perceived benefit against an unclear, invisible threat to privacy (Maurer, Balke, Kulathuramaiyer, Weber and Zaka, 2007). This behaviour has also been identified in users’ online spending habits (Berendt, Gunther & Spiekermann, 2005).

### 2.4.7.1 Privacy Modelling and Tags

Central to the concept of privacy is control over the flow of a user’s information, either from the user (collection of information) or from one system to another (reuse of information). This is by far the most difficult aspect due to the value of the information and the ease with which it is redistributed. This redistribution of information is also far more likely to result in it crossing natural borders of privacy (Langheinrich, 2002). This reuse of information is being addressed with the use of information tags, which limit its use and redistribution.

Jiang and Landay (2002) describe a theoretical model for privacy control in context-aware systems based on a core abstraction of information spaces. This seeks to support the authors’ previous work on a socially based system, and adds the use of privacy tags to describe (using meta-data like tags) how specific information can be accessed or redistributed. The tags are used by the administrating entity to manage access to and control over information within an intelligent environment. Information spaces have been used to respect natural borders of information, and the authors seek to minimise information crossing these borders (unintentionally or otherwise). Information spaces can be described as a 5-Tuple (Objects, Principles, Boundary of space, Operations and Permissions). This list describes the space, its inhabitants (objects and principles) and the way they can interact within the information space. The information contained within these spaces is controlled via ‘unified privacy tags’ (Jiang & Landay, 2002). These privacy tags contain:

- a Space Handle specifying which information space the information belongs to,
Chapter Two: Background Literature

- a Privacy Policy that represents permissions specified by space owners for different types of operations (e.g. promotion and demotion), and
- a Privacy Property List describing an object’s lifetime, representational accuracy, and capturing confidence.

These tags make up the framework for the privacy rules used to determine whether someone has access to a particular piece of information. For example, a DJ could provide the crowd with a free sample of his music, tagged to limit its redistribution or specifying an expiry data when the file would no longer be playable. However, this system does assume that all software processing the tags is trusted, which can be problematic for large-scale decentralised systems like intelligent environments.

Hengartner and Steenkiste (2003) also note that the assumption is made that these environments are administrated by a single entity, and that sources and intermediate nodes are fully trusted. Given the potential for intelligent environments to be provided by completely unknown entities, and the ability of multiple environments to inhabit the same physical space, this assumption is not one that can be made when developing a scalable intelligent environment architecture. Therefore, while these meta-data tags may be useful for controlling information reuse and distribution in a single environment, it is unlikely to be useful in protecting user privacy in a distributed intelligent environment. The Digital Object Identifier (DOI) System (http://www.doi.org/) uses similar digital tagging and a central repository to track information across a digital network. Developed by the International DOI Foundation, this system allows users to track the migration of a tagged object, for example a webpage. This generic framework provides a structured, extensible means of identifying, describing and resolving the tagged objects. This system may be useful for tracking information provided to an intelligent environment, but prevailing privacy research suggests a better solution would be to limit the flow of information to intelligent environments in the first place (e.g. Jiang, Hong & Landay, 2002).

2.4.7.2 Location Privacy

Location information is particularly sensitive in intelligent environments. The disclosure of a user’s current location may allow a third party to locate the user without their permission, but the disclosure of their past locations is likely to be a much more egregious invasion of privacy. Complete histories of users’ movements could reveal their home address, shopping habits, work place, common socialising locations and even reveal treatment or personal problems by linking the user to a particular location (e.g. a health clinic). Users may, however, wish to share their location with family, friends and work colleges.

Location privacy can be defined as the ability to prevent other parties from learning a user’s current or past location (Beresford & Stanjano, 2003). As systems become more effective at precisely locating a user, more thought needs to be put into the collection and use of this information if user privacy is to be guaranteed. For example, the resolution of a location tracking system could be varied to obfuscate the user’s location. Displaying a user’s location
as ‘Brisbane’ may not be a breach of a user’s privacy, but an exact address like ‘142 George St’ might. The setting of a minimum location information resolution would be an example of setting privacy minimums to safeguard users’ privacy.

User interfaces with the intelligent environment must allow the users to set privacy preferences that can handle the variety of different information sharing situations. This includes the contextual influences on a user’s privacy, including location, context, time, the information requester and the type of information requested. Myles, Friday and Davies (Myles, Friday & Davies, 2003) have addressed this problem with LocServ, a privacy preference manager that uses machine-readable privacy policies and user preferences to automate the privacy management decision-making process.

LocServ allows users to restrict the exchange of their information depending on the organisation making the request, the service offered, and the time, location and context of the request (Myles, Friday & Davies, 2003). The system uses an XML-like language to represent the originator and their intent in an information exchange. This allows the systems ‘validators’ to accept or reject an information request based upon the user’s preferences and standard rules. The information exchanged can be anonymised and further controlled by the user by interacting with their detailed preferences. To ensure the system is not a burden on the user, various default settings and privacy preference ‘wizards’ have been developed.

The LocServ system operates under the assumption that all parties in this simulated environment will abide by their privacy policies, and that user privacy should be protected by default (Myles, Friday & Davies, 2003). The system architecture allows users to elect to share certain information, rather than have the users select information to protect. The system is an excellent example of a possible overall goal for intelligent environment development. The emphasis should be on integrating pervasive computing within our environment in a way that supports human interaction without eroding personal freedoms and promoting user mistrust.

Location privacy is often jeopardised via analysis of the interaction logs generated by intelligent environments. Gruteser and Grunwald (2005) demonstrate a method of randomising the user’s mobile device’s MAC address, which prevents the user’s hardware from being recognised from one visit to the next. Beresford and Stanjano (2003) prevent a pseudonym’s movements from being followed from point-to-point (which could potentially be combined with other data to reveal the user’s identity) by switching the pseudonym whilst the user is within an area of high traffic. The concept of ‘Mix Zones’ may also be adapted to obfuscate user’s use of pseudonyms when interacting with ubiquitous computing services, and is integrated into the privacy management solution discussed in section 6.5.3.

2.4.8 Summary and Conclusions

Being socially constructed, privacy is a difficult concept to build into a distributed computing environment. Indeed, modern privacy problems (e.g.
surveillance, identity theft, etc.) make users wary of any system that can automate the collection and inference of information about the user. This makes privacy the most significant impediment to ubiquitous computing adoption, and makes the integration of privacy design from the beginning essential for its success. Individual concepts of privacy evolve in response to the current laws and social norms, expectations of privacy delivered by the market, and the architecture of any computing environment the user interacts with. Given current market, societal and legislative conditions, our architecture must allow users the freedom to explore their own concepts of privacy and interact within those limitations.

Intelligent environments must have limited, clearly defined collection of personal information. This collection must be visible to the user, and where possible they should have control over the use and reuse of any collected information. This may be unrealistic in modern times given the pervasiveness of video surveillance, but attempts to identify users without a compelling reason to do so should be avoided. Feedback on data collection should ensure the user has comprehension, consciousness and control, that the user has given consent to all information collection activities (Patrick & Kenny, 2003), and that the user has access to the intelligent environment’s privacy policies. Information collected or inferred about the environment’s users should, where possible, be restricted to that environment, and should not be allowed to cross any natural borders of privacy (Langheinrich, 2002).

Intelligent environments should avoid active collection of user information through environmental sensors, especially when it occurs without the user’s consent. If contextual information is used to personalise services, it should focus on the interaction and not on sensed details about the user or their handheld device. Service-based intelligent environments should not double as security systems, and active sensing of users’ information should occur only in special, well defined environments (e.g. emergency rooms, aircraft hangars, etc.) (Langheinrich, 2002). Intelligent environments that provide benefits to the user without invading their privacy will be much more useful than the traditional security and sensing environments being developed at present.

Identity Management is an extremely important aspect of user privacy, so much so that the control of the interaction personae used in an intelligent environment (or other system) is essentially the control of a user’s privacy. Users have demonstrated that they want to control the way they are perceived by the real world (e.g. selective use of ‘Faces’ (or persona) to represent a conditional identity to a particular group). This allows users to selectively measure the privacy risks of using a particular persona and maintain similar interactions with the digital world that they enjoy with the real world (in terms of anonymity and the use of pseudonyms). This requirement is compounded by the fact that intelligent environments can be untrusted, and therefore potentially malicious systems. How we handle identity will determine the effectiveness of privacy within intelligent environments, and this ultimately will determine whether intelligent environments will be a success or failure.
Intelligent environments should use certified centralised third party identity authorisation entities to verify user's assertions of identity. These entities provide intelligent environments with a reliable method of confirming a user’s identity without requiring that the user previously sets up an account with the intelligent environment, and it removes the identity authentication process from a potentially untrustworthy environment and limits the additional information that could be mined from a local identity authentication entity. The use of multiple identity providers would allow the service provider greater confidence in the user’s asserted identity. However, repeated use of the same identity providers (even if the identity account numbers are obfuscated, e.g. using the a third party router like the Mist Router (Campbell et al., 2002)) could be used to identify the user between interaction sessions.

By separating service delivery from identity management, it also prevents the combination of vast quantities of service usage data with the user’s personal information, something that consumers have widely rejected in the past. Of course this means that the dissertation’s architecture must address the middle ground normally provided by local identity management and service personalisation. This dissertation’s architecture must identify where local information is required for service personalisation, and determine how this information can be collected and used for maximum user benefit whilst maintaining the user’s required levels of anonymity.

Our interaction with most everyday tools relies on our use expectations that we form from previous usages, and the trust we have that the product will perform as we expect. In the absence of any prior usage or existing trust relationships, we innately rely on the object’s reputation. Intelligent environments will be no different, nor will the use of the tools that allow us to interface them. User must have confidence that their mobile device will only share information in accordance with their privacy preferences. However, it is not practical to expect that one reputation or trust system could provide reliable feedback for all intelligent environments (and their services).

Trust in ubiquitous computing environments works in a similar manner to the trust in the real world. Intelligent environments can require verifiable identities or payment for services, and users must the determination as to whether the risk of interacting with the entity is worth the expected benefits. The main difference between the Internet and intelligent environments is the physically located nature of the services provided by the intelligent environment. This physical location reduces the ability to provide services to any user wherever they are situated, but does allow services to be personalised to a particular area and restrict their access to co-located users. Services must enable methods of jump starting trust between the service and the user, and should avoid the situation of the user of the user having to trust the service provider completely before any interaction takes place. To accommodate this service providers could provide services with varying information requirements to allow users personalised or anonymous services.
The nature of trust is fluid, with users continually evaluating trustworthiness as they gather evidence and experience interactions with the services, person or organisations. The trustworthiness of an environment and its services are essential to their continued use. Any successful intelligent environment must provide automated tools for users to gather this information and organise previous interaction experiences for the user. There also must be a large enough population of environments, identity brokers and services to allow the user choice. A user may choose to use the sole service provider that is inherently untrustworthy, but in this case they should understand the risks of interacting with the provider, and adjust their behaviour accordingly (for example, by sharing less information).

Trust and reputation systems are much more likely to be successful when their recommendations are focused on a single area (for example, intelligent environments within Brisbane or Eastern Australia), or when recommendations are being drawn from a group that the users are part of (such as ‘Backpackers’ or a local community group). What is important, however, is where these trust or reputation systems integrate into the greater infrastructure. These systems would form one part of the framework that provides users with the information to decide whether or not to use a particular environment or service. The dissertation’s architecture will identify the role for trust and reputation systems within intelligent environments, and will make recommendations for their implementation.

The fundamental concern of users within intelligent environments is the management of their information to receive services with as little risk to their privacy as possible. This can be described as giving users the awareness of what information collection is occurring around them (i.e. generally improve the information flowing to the data owners and reduce the information flowing to the data collectors or data users), allow them to provide information to receive a service of value (ideally in an opt-in method, rather than an opt-out default position), and allow users to vary what information (and its accuracy) is provided to the service.

Location is important for the control of information within intelligent environments. Intelligent environments must control a user’s location information to prevent current and future breaches in the user’s privacy. Intelligent environments also require a method of stopping information from flowing unexpectedly across the natural borders of privacy. The use of privacy tags or metadata labels has been suggested to manage the sharing of information, but these systems require that, for all software handling the information is trusted, something that is unlikely within a widely deployed intelligent environment infrastructure. These systems could be developed using trusted computing components (refer to section 2.5.2.2), but these would most likely be limited to individual intelligent environments that their users have reason to trust (e.g. the environment is served by the user’s employer).
2.5 Security

The essence of good security engineering is understanding the potential threats to a system, then applying an appropriate mix of protective measures – both technological and organizational – to control them. (Anderson, 2001)

Effective security is essential for user privacy in so far as security within an intelligent environment prevents unauthorised access and exploitation of information and intelligent environment resources. Security concerns within intelligent environments include not only eavesdropping, but also masquerading, tampering and denial of service (Coulouris, Dollimore & Kindberg, 2001, p. 251). These dangers to security are countered with appropriate application of cryptography, effective system design and the use of digital certificates to create trust among users and organisations (Coulouris, Dollimore & Kindberg, 2001). This section reviews the basic security concepts that are used within the dissertation, and considers what specific security concerns are created through the use of ubiquitous computing technologies.

Traditional methods of security are not always appropriate for ubiquitous computing environments. The physical availability of components can cause significant risks to the environment’s security as they can be hacked, broken, stolen or prevented from conserving battery power (and thus drained of power) (Campbell et al., 2002; Stajano, 2002). Other limitations on security in ubiquitous computing environments include limited processing power, wireless communication bandwidth and battery size. The level of security required within intelligent environments is often dependent upon its purpose. The processing of banking and medical records in particular requires more sophisticated security than, for example, the exchange of phone numbers across an ad-hoc mobile network.

The invisibility of ubiquitous computing environments can also have an impact on their security. It is often difficult to determine when traditional computers are transmitting information to the Internet, and this problem will only increase with ubiquitous computing (Stajano, 2002, p. 49). This not only highlights the need for the effective security of ubiquitous computing environments, but it also underscores the need for more descriptive feedback on the exchange of information. This section describes the basic components of security in ubiquitous computing and evaluates current and ideal security design in distributed computing environments.

2.5.1 Ubiquitous Computing Security

Security in distributed ubiquitous computing environments is defined by three fundamental security properties: Confidentiality, Integrity and Availability (Stajano, 2002, p. 4). Confidentiality is the property that is violated whenever information is disclosed to an unauthorised principal. Integrity describes the delivery of a message without its being altered. Availability describes the property of a given system to always be available to honour requests from authorised principles. Finally, Authentication, the process of verifying a principal’s claimed identity, is examined to develop an understanding of the
identity authentication that is essential in creating trusted links between parties.

2.5.1.1 Confidentiality

Confidentiality is the property that information holds when it remains unknown to unauthorised parties. When information is inappropriately passed outside of the controlling organisation, the threat to confidentiality is called disclosure (Stajano, 2002). The unauthorised use of the data in the storing organisation is called a (unauthorised) ‘use’, while a breach contrived by an outsider an (unauthorised) ‘access’. The entity whose confidentiality needs protection typically assumes the form of a message, that is, a sequence of bits that is transmitted between two entities. Confidentiality seeks to keep the message a secret from any third parties that may, even legitimately, handle the message in its transmission from the sender to the recipient. Confidentiality is required not only for messages in transit, but also for messages held on a device or storage peripheral and for any metadata (e.g. who, with whom and when) describing each message as well (Stajano, 2002).

Confidentiality normally relies on the use of encryption to obscure the message. A cipher is a pair of complementary algorithms: one for transforming the plaintext into an encrypted message (encryption); and one for decrypting the message back to plaintext (decryption). Different methods of encryption involve the use of differing ciphers and network architectures, and must be tailored to the individual network’s circumstances (e.g. clock speed, battery power etc.). Generic intelligent environment architectures must accommodate all interaction requirements or limitations in available hardware when securing users’ information, e.g. limited processing or battery power.

True confidentiality from cryptographic ciphers comes from their strength, and not by obfuscating the encryption algorithm used. Whilst being unaware of the cipher may in some cases add an additional layer of obfuscation for the message, the benefits gained from using a widely used and tested algorithm far exceed those from obfuscating the cipher’s origins. That is, it is much better to use an algorithm that has had the benefit of peer reviewal by competent cryptographers (Stajano, 2002). Intelligent environments should therefore use a widely accepted, accessible algorithm rather than a potentially less secure, unknown algorithm.

There are two basic types of encryption keys: symmetrical and asymmetrical keys. Symmetrical encryption (also known as Secret Key Encryption) is a method by which data is encrypted with a single key (shared secret) and can be decrypted using exactly the same key. Asymmetrical Encryption (also known as Public Key Encryption) is a method by which data is encrypted with a single key (nominally called the Public Key) and can only be decrypted with a different related key (nominally called the Private Key). Public Key cryptography was developed by Diffie and Hellman (Diffie & Hellman, 1976), and was further developed in (Rivest, Shamir & Adleman, 1978).

The benefit of symmetrical encryption is that it is highly efficient, reducing the time and computational effort required to encrypt/decrypt data. The major
drawback is that it requires some secure means of exchanging keys with the user's correspondents before it can be used. Further, if users want to have one shared secret key for each correspondent, then they will be required to keep a large number of keys. These drawbacks are overcome by using a security architecture that manages key distribution and access to network resources, such as Kerberos, described in section 2.5.3.2.

The benefit of asymmetrical encryption is that it eliminates the problem of key distribution because all participants simply publish their keys (Rivest, Shamir & Adleman, 1978). It also eliminates the problem of key management because there is just one public key for each party located in one central place. The drawback is that this form of encryption is highly inefficient, meaning that it takes a standard computer a relatively long time to perform a small encryption. This inefficiency is normally addressed by using a combination of public/private keys to exchange information. An example of this is Pretty Good Privacy (Zimmermann, 1995a, 1995b), which is described in section 2.5.3.1.

Traditional public key cryptographic schemes use numbers that are hundreds of digits long, not something a human being can remember easily. Even elliptic curve cryptographic keys are several tens of digits long (Boneh & Franklin, 2003). Cryptographic systems put these keys into a data structure called a certificate that includes a text string humans can use to identify the certificate. Identity-based encryption is a relatively new encryption scheme that can produce a public/private key pair from any string. The use of a string makes the public key easier to remember and allows a standard method for generation of private keys. In identity-based encryption, the actual key is a function of a text string itself. This method allows messages to be encrypted and sent before the private key has been generated (Boneh & Franklin, 2003).

The confidentiality of a message can be compromised in several ways. Older, simpler encryption ciphers can be overcome with a brute force attack, which tries every combination of possible decryption keys and looks for a plaintext result when applied to the secured message. In such an attack, the possible keys, ranging anywhere from 40 to 1024 or more bits long, are divided between multiple processors, and the result of applying them to the secured message is evaluated. An instance of this occurring was the 1997 RSA Data Security challenge when a collaboration of about 70,000 machines across the Internet was utilised to crack a 56-bit DES (Data Encryption Standard) key, in use since 1977 (RSA Data Security, 1997). When using encryption ciphers, the longer the key the less chance that a message can realistically be decrypted. The use of long cipher keys can prove to be computationally expensive, especially for the simple processors commonly found in ubiquitous computing environments, but the threat of the encrypted messages being intercepted and decrypted on powerful machines cannot be discounted (and therefore encryption must be based upon these threat profiles).

The current ciphers available today use upwards of 256-bit keys and are for all practical purposes unbreakable (Stajano, 2002) using existing computing systems. When evaluating communication confidentiality, we must evaluate
what key pairings are to be used, how these can be distributed and what devices will actually be involved in the encryption. Asymmetric keys (e.g. the widely deployed RSA public key cryptosystem (Rivest, Shamir & Adleman, 1978)) allow the use of a public key to encrypt a message (encryption \( C = M^e \pmod{n} \)) and the use of a secret private key to decrypt the message (decryption \( M = C^d \pmod{n} \)).

The current encryption standard is the Advanced Encryption Standard (AES) (Coulouris, Dollimore & Kindberg, 2001), which mandates the use of a particular algorithm using a 128, 192 or 256 bit encryption key. AES provides stronger encryption than previous schemes (e.g. Temporal Key Integrity Protocol (TKIP)). AES is also able to fulfil government encryption requirements, which puts it on par with tough encryption schemas such as Triple-DES (which uses the DES algorithm to encrypt the package three times using different keys) (Bort, 2003). AES key lengths are likely to be extended in the future as more powerful computers become able to defeat these algorithms using brute force attacks.

Confidentiality of information provided to a service provider or organisation is also at risk when the information is being processed, and when the information is stored on storage media. The processing of information remains the greatest challenge of the two, as the service provider is unlikely to be a trusted entity. To address this risk information shared with the service provider should not be something the user is unhappy being inappropriately disclosed (as the risk of this is very real). Identity broker numbers and information that could be used to identify the user should be provided in a manner that doesn’t allow the service provider access to it. This could be accomplished, for example, but encrypting the account information with the user's or identity broker's public key.

The confidentiality of stored information examines the risk of unauthorised access. This is of particular concern when using ubiquitous computing environments that may be physically vulnerable. To overcome this information should be encrypted when stored on local storage media. Trusted Computing components can also be used to ensure the same configuration of the service provider hardware and software is present during the access, which prevents the ‘spoofing’ of the service using similar components when attempting to decrypting the stored information.

The types of collusion attacks possible in intelligent environments are explored by Molnar and Wagner (2004) in their study of the privacy and security issues surrounding RFID tag tracking architectures. In the Molnar and Wagner (2004) study, the item-level RFID tagging used in libraries to track books is equivalent to tracking users within an intelligent environment. In this architecture, it was determined that no information should be placed on the tag, beyond an identification number secured to prevent tracking or ‘hotlisting’. By preventing the passive gathering of identifiable information by third parties, the authors show how this architecture can avoid collusion attacks and passive eavesdropping by encrypting communications and securing all information within the environments (Molnar & Wagner, 2004).
The library RFID tracking system demonstrates the benefits of a centralised system that allows the identification of each item by the system (perfect for a library or centrally managed system). It does not, however, allow for private interactions with potentially untrustworthy environments, nor does it eliminate dangers of collusion attacks from multiple intelligent environments, and leads the user open to being tracked via system logins. This method of passive information gathering should be avoided in any privacy aware system, particular in ubiquitous computing environments where the potential for harm is much greater than in typical computing systems. User information should be stored in specific user controlled and (non-environmental) third party entities, and should be encrypted for storage or transmission.

### 2.5.1.2 Integrity

Integrity is the property that data holds when it has not been modified in an unauthorised way (Stajano, 2002). When data is modified, to other meaningful data, it can be said to be corrupted. This corruption is more likely to be caused by malice than by accident, and this act of corruption may be more damaging than outright theft of the data. Integrity is independent from confidentiality, as it allows both parties to verify that the message has not been corrupted, and is therefore of great importance in ubiquitous computing environments when using financial or identity-based services. Integrity is verified through the use of error-detecting codes, which seek for bit-errors caused by random noise or malicious third parties, and digital methods of signing data, like Hash functions, digital signatures and message authentication codes.

Cryptographic hash functions are one-way functions that compute a unique hash of any data to the size specified by the algorithm, e.g. 256 or 512 bits for the Advanced Encryption Standard (AES). This function is a one-way function that anyone can use to verify a message’s integrity by hashing the plaintext message and comparing the hash function with that sent with the original document. If they match, then the message’s integrity is assured. It is, however, possible for any malicious attacker to recompute the hash function for the new message and substitute it into the new message. As digital signatures and the message authentication codes are only creatable by the message’s originator, they are capable of withstanding this sort of attack (Stajano, 2002).

The message authentication code is a bit like a hash parameterised with a secret key, with each key applied to the message authentication codes giving a different hash function. This allows only those with the secret key, shared as part of an initial handshaking connection in any given environment, to create and verify the hash result. This function, therefore, requires a mechanism for the sender and receiver to establish a shared secret (Stajano, 2002).

Digital signatures are an attempt to recreate the defining characteristics of a person’s written signature, namely that (at least in theory) no one else can generate it, and that anybody can verify its authority. Digital signatures are therefore useful for signing electronic documents or messages when the
exchange of a shared secret between the sender and the receiver is infeasible or undesirable. To avoid simple digital recreation of the signature, it is developed from the document or message that is to be signed. The use of digital signatures assumes the availability of public key ciphers, and was first suggested by Diffie and Hellman (1976) and implemented by Rivest, Shamir and Adleman (1978).

A digital signature is created by using the users’ private key to produce a decryption bijection that is unique to the signed message. This signature can be verified by the reverse operation with the user’s freely available public key. It is possible to encrypt and sign messages using the same algorithm, but using separate algorithms and keys for either task prevents additional risks like the ‘chosen protocol attack’, in which a third party runs a challenge response protocol with you in an attempt to make you sign a message without your knowledge (Stajano, 2002). A convenient way to enforce separation is to have different key pairs for encryption/decryption and for signature/verification.

The use of hash functions in an intelligent environment gives no guarantees of a message’s integrity, as it may have been faked and the hash value recalculated by the forger (Stajano, 2002). The message authentication code function can be used, assuming the secret key has remained secret, to verify that a message is genuine, as no one else could create the authentication value. This, however, does not allow the transfer of this belief to another party that does not have the shared secret. Moreover, if three or more people share the secret, then the receiver cannot be certain that the message was not altered in transit (Stajano, 2002).

Digital signatures, however, are able to create non-refutable signatures, as the key that makes the signatures is never shared with anyone. This allows the receiver of a message to confirm its sender’s identity by comparing the signature with the public key hash of the message. This property of digital signatures ensures that, once signed, users cannot deny they have signed the document. This is referred to as non-repudiation, and it is an important property in the development of trustworthy computing environments.

Digital signature schemes depend upon the public key of the message-sender being available to the recipient. The most practical methods of doing this involve including the public key in the message, storing them on a readily available (privately managed) server, or placing the public keys in one or more centrally managed directories (Clarke, 2001). An intelligent environment could therefore have a central repository for public keys of all users interacting with the environment. However all of these methods are subject to ‘spoofing’, and therefore are not appropriate for important message exchange (like identity authentication or some service delivery).

A ‘certificate’ us a digitally signed, structure message that asserts an association between specific data (an identifier) and a particular public key (Clarke, 2001). An ‘identity certificate’ is then a particular class of certificate that associates a particular identifier with a particular key. Traditionally, a certificate needs to be created by a trusted ‘public key certification authority’
which verifies the user’s identity and digitally attests to the identity by signing the certificate using the CA’s own private key. This creates a train of trust that can be reference back to the CA, but the process is lengthy, and does not allow the ad hoc creation of trust relationships (Clarke, 2001).

Private keys are therefore essential to the creation of signatures and certificates that help demonstrate and transfer trust. But private keys are capable of being compromised, which would undermine the entire chain of trust. It is therefore vital that an efficient and effective method of revoking certificates and their associated key-pairs exists. Interactions within an intelligent environment will use digital signatures for messages within the environment (where interactions are likely to be anonymous, and therefore new security key pairs can be used for each interaction). Identity authentication within in the intelligent environment will need to ensure the provider is who is claimed, and therefore certificates will be used in communicating with the identity providers.

The different mechanism selected for ensuring integrity is obviously context dependent. In ubiquitous computing environments, often there are situations where multiple sensors would want to connect with a user’s mobile device. In this situation no shared key is possible, as there is no one entity to communicate with. Instead, these devices can be certified by a reputable third party which could then sign each of their transmissions. Receivers of this information could then verify the signature using the public key in the certificate, and their computer could verify the public key of the reputable institution, which it would know axiomatically in the same way as your web browser knows the public key of Verisign (Stajano, 2002).

This may be a problem if, for example, the individual sensors or computing devices are unable to handle the computational cost of the public key operations. A temperature sensor might not have the computational ability or power to digitally sign each of its readings. This limitation is a necessary design consideration of all intelligent environment designers. The use of more computationally advanced devices as data-clearing houses might allow information from simple sensors to be reliably distributed. In many instances, it may not make sense to provide this security, e.g. for temperature gauges.

The physical availability of intelligent environment components makes them vulnerable to tampering. This tampering could be overt, as in the changing of a sensor’s software to make it provide false information, or covert, for example the continual interaction with a small device to exhaust its battery power and remove it from its usual duties (described below as ‘Sleep Deprivation Torture’). Ubiquitous components could be secured using a Trusted Computing base (see section 2.5.2.2), but this may be too expensive or computationally unfeasible given the design of the components. Another option for low-cost devices would be to make them tamper-evident, where a device would simply be discarded once evidence of tampering was discovered (Stajano, 2002, pg. 129). Hardware-based encryption chips can also be used to reduce encryption time (McLoone & McCanny, 2001), and they could be used in ubiquitous computing environments to allow more efficient use of
resources (both in terms of clock cycles and battery power) (Stajano, 2002, pg. 110).

Not only must the communications between users and service providers be immutable, but there must also be ‘integrity of service’, or the guarantee that the service will behave as expected (or as described by the service descriptor). Services must not only be available (see next section), but they must also collect, process and retain data as expected is users have any change of accurately judge the impact of a service interaction on their privacy. This dissertation’s intelligent environment architecture must therefore have accurate service descriptors that can be provided to the user before they connect to the service.

2.5.1.3 Availability

Availability is the ability of a system to perform its advertised service in a timely fashion when requested to do so (Stajano, 2002). Attacks on this ability seek to deny service to the system’s users. While confidentiality and integrity are essentially concerned with ‘what a user is allowed to do’, availability is concerned with ‘what a user is able to do’. The nature of distributed computing provides numerous challenges to a system’s availability, including its data management, fault tolerance and failure recovery, file naming (Anderson, 2001), and the threats of mobile code (Stajano, 2002).

Concurrency describes the running of two or more processes at the same time. This gives rise to problems when processes may use old data, lock databases whilst updating them (preventing accessibility), provide near simultaneous conflicting updates to the database (rendering it unusable), and provide poor time security for time-dependent authorisation protocols (e.g. Kerberos). These common problems are considered when developing the intelligent environment architecture.

Fault tolerance and failure recovery are important aspects of security engineering (Anderson, 2001). System failure is overcome by implementing system resilience and a level of redundancy for the system to revert to in the case of failure. Intelligent environments might, therefore, have multiple beacons for broadcasting services, use virtual machines on separate hardware to manage user interaction and where possible separate the intelligent environment’s main access point from the services it provides.

Denial of service (DoS) or Distributed Denial of Service (DDoS) attacks describe attacks where (either legitimate or illegitimate) users, whether through malicious or accidental designs, consume sufficient system resources to prevent other users’ access (Stajano, 2002). DoS attacks do not normally involve illegitimate users as they are normally stopped from accessing the system through the standard access control mechanisms. Public intelligent environment service providers however may have no access control, and would be especially susceptible to these attacks. DoS and DDoS attacks can be difficult to repel, but expensive attack deflectors can be used to determine the origin and block these attacks. A suggested method of reducing or preventing denial of service attacks involves users pledging (to be forfeited if
they act dishonestly) or paying a small sum of money (or another resource) each time they access the system (Stajano, 2002, p. 136).

Another DoS attack is the threat to the limited battery energy of the micro-devices that make up ubiquitous computing environments. These devices (typically sensors or simple network nodes) normally have a waking/sleep routine that can be interrupted by malicious or serendipitous use. This attack is also called sleep deprivation torture (Stajano, 2002), and could be exacerbated by the physical access to a device (and its power supply) that exists in many ubiquitous computing environments. This attack can be defeated with effective battery management and resource reservation, and through the use of mains power and tamper resistant (or tamper evident) components (Stajano, 2002).

File naming can also be a problem in massively distributed computing systems, as the number of potential users grows beyond that which can be readily managed and shared. This problem is further exacerbated when user names are used for identification, as there are few truly unique names in the world. This problem is unlikely to present too much of a problem within intelligent environments, as users will likely be physically present, and unique random numbers would be used for identification to maintain user privacy. These design considerations are taken into account during the development of our intelligent environment architecture.

The final threat to system availability is that posed by malicious mobile code (or viruses). This threat is a symptom of the current virus culture that exists in traditional computing, and of the mobile intelligent agent infrastructures that are being developed as intelligent environments (Coen et al., 1999). Methods of avoiding this threat involve the running of a timer along with any process executed by mobile code which monitors the code and prevents it from consuming excessive resources or accessing protected system components (Stajano, 2002). Further evaluation and design of a technical solution to this problem is outside the scope of this research.

### 2.5.1.4 Authentication and Authorisation

Intelligent environments provide information and service access to users within their physical environment. The information exchanged within these environments is most likely to be of limited size and complexity (i.e. a user profile, service interaction preferences etc.). These information exchanges are easily encrypted and digitally signed providing adequate confidentiality and integrity. It is, however, difficult to manage and confirm the identity of users within ad-hoc or new intelligent environments, and this usually implies some prior relationship or configuration. This architecture attempts to provide identity authentication without requiring a prior relationship with an intelligent environment.

Security in intelligent environments is comprised of two parts: Authentication and Authorisation (Tuchinda, 2002). Authentication is the process of verifying an assertion made by a user. The assertion could be an assertion of identity (Identity Authentication) or of a particular attribute or information (Attribute
Chapter Two: Background Literature

Authentication). It is the logical step after identification, that is, establishing who that principal claims to be (Stajano, 2002, p. 75). The process of identity authentication is described in section 2.4.4.

User (identity or attribute) authentication is based on three main verification principles:

- something the user knows (e.g. a password),
- something the user has (e.g. a key, a certificate, etc.), and
- something the user is (e.g. finger prints, retina, etc.).

This list is not exhaustive, however, as new methods for uniquely recognising users are developed. A novel method of user authentication involves asking users to recognise photos from their own digital media collection amongst a group of stock images (Pering, Sundar, Light and Want, 2003). Biometrics has evolved to allow the use of not only facial or fingerprint recognition, but the use of voice, hand shape, pheromones and even recognising dance moves. Other potential methods include ‘what you do’ (i.e. keystroke analysis) and ‘where you are’ (particularly important for context-aware intelligent environments) (Gollmann, 1999). Users interacting with intelligent environments must therefore be able to prove their identity using one of these five authentication methods.

A common method of identifying a computing device is through its Media Access Control (MAC) address. MAC addresses are standard labels that identify a media device (e.g. a network card) whilst interacting with a network. Under normal conditions, when a device connects to a network it would be identifiable by this address, allowing different interaction sessions to be linked together, potentially allowing a detailed picture of the device’s usage to be developed. Methods of ensuring the privacy of these addresses, that is, by using randomly generated MAC addresses (Gruteser & Grunwald, 2005), prevent this association. Similar techniques must be utilised to maintain user privacy when moving between multiple intelligent environments to prevent logging of their interactions.

There are several concerns about authentication over non-secure networks. Authentication that simply relies on the exchange of a password might be subject to replay attacks if the password is transmitted in the clear (without encryption) or if the encryption channel is compromised. To defeat replay attacks, an authentication system must ensure that the authenticator that is currently required cannot be predicted from previous ones (Stajano, 2002, p. 77). The next logical authentication step from this point was the development of one-time passwords, with a batch of passwords generated prior to their use. This has the problem of requiring storage of all potential passwords (and their order of use, or their ‘state’ of use) in the server, and of course requiring a pre-existing relationship with the authorising entity. Additional connection mechanisms should be used to set authentication timeouts to improve security (including setting Maximum Session Times and Session Inactivity Timeouts).

All of these methods also imply the use of a central server for the authentication of the credentials supplied by the user. Whilst intelligent
environments could have this functionality, it would only be realistic in environments that have a pre-existing relationship with their users. Intelligent environments that are designed to be used either in an ad-hoc manner or anonymously need a method of authenticating communication with another party without these pre-existing relationships. In addition, the storage of passwords on a central server raises other security concerns. Hardware that is accessible to the public (a situation that is common in ubiquitous computing environments) may lead to hardware theft or hacking to recover user names and passwords (even if standard methods of securing passwords on a server are taken, for example hashing the password or ‘salting’ the password with random characters to frustrate pre-computation of passwords. (Morris & Thompson, 1979; Stajano, 2002, p. 76)).

Authentication of an identity or attribute assertion can be performed in a stateless manner using a ‘Challenge-response’ protocol exchange with an identity provider. In this protocol, User $M$ sends a random number $n$ which User $A$ must return encrypted under their shared secret key $K_{AM}$. This method prevents replay attacks, as a new random number is sent each time, but is susceptible to man-in-the-middle attacks that provide the same challenge to another member with the shared key (and replaying the response to the original challenger) (Anderson, 2001, p. 19; Stajano, 2002, p. 78). Simple authentication involves the addition of a ‘nonce’ or ‘number used once’ to the message before encryption, which allows the receiving party to decrypt the message and the nonce, and confirm that it has not been used before (i.e. that a replay attack is going on). These nonce numbers could be random numbers, a serial number, or a random challenge received from a third party.

The Needham-Schroeder key distribution protocol (Needham & Schroeder, 1978) provides a method of securely distributing private keys between network entities (or users). It uses ‘nonces’ in the exchange of information between users to allow users to check for replay attacks, and creates ‘chains of trust’ between users when transferring session keys. This protocol explicitly assumes all participants behave themselves, and that attacks only come from the outside (Needham & Schroeder, 1978). This is unrealistic in modern distributed systems with untrusted participants and potentially anonymous interaction. The Needham-Schroeder protocol also has the problem that the exchanged keys are non-revocable, which allows keys compromised over time to still be used, and any keys distributed using the compromised key might then also be compromised (Anderson, 2001). This may especially be a problem if short encryptions keys are used and then later decoded by increasingly more powerful computers in years to come.

Kerberos (Neuman & Ts’o, 1994; Steiner, Neuman & I., 1988) is an extension of the Needham-Schroeder protocol that utilises a central server for key exchange and time-stamped access-tickets to manage revocation of access rights. Kerberos uses two levels of authentication: a central system to which the user logs on, and a ticket-granting system that gives them access to various resources (e.g. files, services, etc.) (Anderson, 2001). Kerberos uses time-stamps (instead of nonces, like the Needham-Schroeder Protocol) to allow participants to avoid replay and man-in-the-middle attacks, while the
encryption keys used help prevent message changing attacks and maintain confidentiality. This protocol is vulnerable to attacks and chance errors adjusting the central server’s clock time, which may cause real shared keys to be rejected, or old keys to be mistakenly approved. This vulnerability is magnified when considering the greater physical access to tampering provided by the situation of ubiquitous computing hardware in their local environments. The benefits and disadvantages to using the Kerberos system are described in section 2.5.3.2.

The security of the intelligent environment hardware must focus on both preventing physical tampering and maintaining the integrity of any link to the environment’s master clock. Given the localised nature of our intelligent environments, maintaining a local clock for security and information logs that is referenced when a user joins an environment may help reduce these threats (although there may need to be an additional check to ensure that the time used does not vastly differ from the one on the user’s device (as this would suggest this vulnerability may be increased)).

Further work on authentication within ubiquitous computing environments has focused on the unique nature of the hardware (its ever reducing size, limited battery and computational power, physical accessibility of the hardware, etc.) and the inclusion of untrusted or uncontrolled resources in the environment (i.e. potentially untrustworthy sources of data from insecure sensors). Stajano (2002, p. 88) describes the process of ‘imprinting’ devices to maintain recognition of their master controllers, and suggests designs that prevent a relatively simple node from being compromised without its masters knowledge. This level of security management, including trust and information exchange at the sensor level, is beyond the scope of this thesis.

Authorisation ensures that an identified user has access only to resources that they have been authorised to use (Tuchinda, 2002). Access control is a mechanism in the authorisation process that determines who may access certain resources and under what conditions. Access control on an operating system typically authenticates principals using some mechanism such as passwords or Kerberos, then mediates their access to files, communications ports and other system resources (Anderson, 2001). Identity and attribute authentication is described above.

Access control is much simpler when a system’s information and users are known ahead of time and these relationships can be defined in a central server. Intelligent environments are inherently unbounded and require a degree of scalability. A centralised authority managing access control therefore would not be appropriate (Kottahachchi & Laddaga, 2004). An environment’s typical binding to a particular location means access decisions must be locally relevant, and the system be extensible to allow the mechanism to react to new conditions and requirements.

Access to restricted services is often restricted not to particular identities, but often to identities that have authorisation to act on behalf of an organisation or association (collective). This requires authentication of an assertion of agency, which follows the same process as identity authentication. These
groups are often imaginary ‘incorporated’ bodies, so the challenge in this instance is that these groups have no corporate form to which to ‘bind’ a signing key. In this dissertation we consider the user that is acting as an agent for a corporation to be this ‘entity’, but the challenge of interactions of these nature is outside the scope of this research.

Of particular concern in intelligent environments is the ability of malicious third parties to conduct inference attacks on their service provider or user register databases. Intelligent environments could be particularly susceptible to these attacks as information is collected by the attackers from poorly or unencrypted exchange of information within the environment, stolen from hacked sensors or gathered through social engineering (from users within the physical environment). Access control must therefore be vigilant against these attacks and prevent user information being stolen through phoney service calls and environment interactions.

Hengartner and Steenkiste (2003) describe three general rules to address the difficulties of applying access control to the information gathered in pervasive computing environments. These design principles for these computing architectures are: 1) extract pieces of information in raw data streams early, 2) define policies controlling access at the information level, and 3) exploit information relationships for access control. Access control also needs to be considered for an entities context. When running access control checks, we can use two types of checks, the End-to-End model and the Step-by-Step model (Hengartner & Steenkiste, 2003). In the End-to-End model, the source node identifies an authorised sink node, and all nodes between the two are authorised to receive the information. This is more efficient but, as all nodes are authorised at once, is very susceptible to denial-of-service attacks. In the step-by-step model, for each possible pair of server/client nodes, the server node validates whether it should give information to the client node.

Hengartner and Steenkiste’s access control architecture uses a policy description language for the specification of policies controlling access to information. This language should be flexible (allowing access control to, for example, individuals or groups) and allow the implementation of other constraints like time (and the information’s and user’s context or physical location). Policies controlling information within pervasive computing environments should therefore operate at the ‘information level’ (Hengartner & Steenkiste, 2003). This allows the users to set high-level information control policies without needing to know the architecture. This language will help in the defining of policies controlling access to information and in automatically deriving access control policies.

The Management of Authorization for site Policy (MAP) system (Zurko & Simon, 1996) provided tools to support policy-oriented operations on a site’s underlying authorisation mechanism. This prototype augmented an existing Access Control List (ACL) mechanism with sensitivity labels, object groups and access rules. This provided a flexible method of assigning labels to information relationships (flows), which proved to be superior to the inflexible Role-Based Access Control model (Ferraiolo, Cugini & Kuhn, 1995), which had trouble handling non-permanent objects. Tuchinda (2002) extends role-based
access control with additional contextual labels for information, for example, ‘time context’ and ‘location context’, and the dynamic setting and revoking of permissions. This extends the system to consider emergency access and user privacy in information sharing.

Not all access control needs to tightly regulate access to the system’s information. Many systems could benefit from a more relaxed approach, especially if the information protected is not overly sensitive. Povey (1999) describes the terms Optimistic, Pessimistic and Mixed security as methods of ensuring user privacy and proactively managing information exchanges. Optimistic security assumes that there will be few breaches in security, and therefore management and recognition of breaches occurs after the fact (and action is taken). Pessimistic security checks everything first and action is taken before a breach occurs. This uses more resources. A mixed approach uses user preferences to manage which exchanges fall into either category. Optimistic security employs social pressure to achieve self-restraint, and simple technical means and ex post-facto redress to prevent unauthorised access, instead of creating complex security and access control policies upfront (Iachello et al., 2005).

A final approach that has been suggested seeks to reduce the burden of administration of access control in cases where users could gain an advantage by having numerous throw-away identities. This could be the case where reputation is important, for example on an online auction site, where the user could simply create another identity to avoid previous poor feedback and continue acting poorly without concern. Plutocratic access control calls for users to pay a small fee every time they set up a new account or service access (Stajano, 2002, p. 136). The fee should be small enough to be negligible to legitimate users, but large enough to make the setting up of numerous identities for nefarious purposes infeasible (or at least less likely).

2.5.2 Security Design

Whilst given unlimited time or resources all encryption is vulnerable, for all practical purposes modern encryption algorithms are unbreakable (Stajano, 2002). But effective encryption only addresses one aspect of security. Anderson sums this up with the statement: ‘Anyone that thinks security is all about encryption doesn’t understand encryption, and doesn’t understand security’ (Anderson, 2001). This section examines other aspects of security design, including security policies, control of access to information and resources, the use of trusted computing and user-centred security.

2.5.2.1 Security Policies

Security policies describe how information should be restricted and what social changes, procedures and technologies are required to enforce these restrictions. A security policy should clearly and concisely express what the protection methods are to achieve, the current threats to security and how these threats should be overcome. This section examines the two most common methods of restricting information: Multilevel and Multilateral
security. These two methods will be evaluated and implemented into our intelligent environment’s design in chapters five and six.

Multilevel security describes the control of data based upon its designated secrecy level (Anderson, 2001). The military uses multilevel security when classifying documents from open, to confidential, secret and top secret. This top-down approach to securing information regulates the way information can be passed within an environment. In the military example, the basic premise is that information cannot flow downward, for example from Top Secret to Secret. This basic premise translates into two enforceable system properties: no process may read data at a higher level, and no process may write data to a lower level (Anderson, 2001). The second property is primarily concerned by attacks by malicious code which could potentially be introduced into a secret database and declassify information by copying it to a lower security clearance database.

Multilateral security involves the separation of particular types of information to prevent breaches of privacy or ethics. Instead of preventing information from flowing ‘down’ security levels, multilateral security prevents information from flowing ‘across’, that is, between departments (Anderson, 2001). This security is required when the flow of information between different entities would be considered a security breach. For example, in a hospital it would be a breach of privacy if a user’s medical records were made available to the hospital’s admin or maintenance staff. An investment bank may have several clients competing in the same field, for example energy generation, and thus have internal rules designed to prevent conflicts of interest.

A common threat to multilevel security, and particularly medical records, is social engineering. A social engineering attack is when a malicious person contacts a person with legitimate access to information and convinces them to provide them with information. This bypasses normal access controls, and has become such a successful method of gathering valuable information illegally that there are people all over the world that make a living in this way (Anderson, 2001). User training and awareness of social engineering attacks are effective ways of reducing their effectiveness. Ubiquitous computing systems may be vulnerable to a similar electronic version of this attack. Users who routinely interact with a service might be tricked into using a fake substituted service that is simply collecting information on its users. A method of ensuring a user’s device can verify the identity of the service is essential to prevent this kind of attack.

The implementation of these security policies is concerned with both how the system’s data are stored and how access to this data is enforced. This research considers multilateral and multilevel security policies when considering how to best secure the data within a ubiquitous computing infrastructure.

2.5.2.2 Trusted Computing

Trusted computing operates through a combination of hardware and software to provide two basic services, authenticated boot and encryption, which are
designed to work together (Felten, 2003). The authenticated boot service monitors what operating system software was booted on the system and provides applications with a way to tell which operating system is running. This is done by adding hardware that keeps an immutable log of the boot process. This allows other programs to tell what software configuration is currently in use and can certify an application’s configuration. Programs interacting with the system can therefore test if it has been compromised through malicious software or other means. This could be used in intelligent environments to detect whether a system has been compromised (physically or via malicious software) if a central repository holding this configuration can be maintained.

The encryption service allows the machine to encrypt data in such a way that it can be decrypted only by a certain machine, and only if that machine is in a certain hardware and software configuration (Felten, 2003). This means that information can be encrypted on a hard drive in a way that makes it unusable to other applications or machines. While potentially useful, trusted computing has garnered significant negative press based upon its potential uses. It will make it straightforward for all sorts of vendors to tie products to each other, to lock applications and data on different platforms, and to tie down licences for the software components of systems to particular machines (Anderson, 2001). An example of this is the authentication printers use to detect non-genuine ink cartridges and either downgrade printing quality or prevent their use altogether.

There is great potential for trusted computing to help secure ubiquitous computing environments. Ubiquitous computing components are often physically accessible, which makes them vulnerable to hacking etc. Trusted computing can be used to monitor the software being run on the component, and action could be taken to quarantine or label compromised hardware. The encryption service could be used for password management and securing information on hardware is physically vulnerable to tampering. Finally, trusted computing can be used to authenticate an environment’s identity, which would prevent the substitution of hardware by a malicious entity attempting to spoof an environment’s service. Using this authentication method, a central list of known (local) intelligent environments could be published, allowing users to confirm their identity when the environment is discovered.

### 2.5.2.3 User-Centred Security

Any user-centred service architecture must adopt a user-centric view of privacy and security. This involves not only considering the user’s privacy during the initial design phase (see section 2.4.2), but also the consideration of how users will use the system and what support will be required to ensure that any security mechanisms are effectively understood and utilised. This focus tries to address the existing problems of users not understanding security models, breaches caused by users sharing or writing down passwords, and usability problems that arise when users have difficulty interacting with the security controls of required systems (Morris & Thompson, 1979). These problems often stem from unclear or poorly
communicated security policies or from poorly designed or unusable security systems. Good system security involves realistic evaluation of the risks not only of deliberate attacks, but also of casual authorised access and accidental disclosure (Morris & Thompson, 1979).

User-centred security refers to security models, mechanisms, systems and software that have usability as a primary motivation or goal (Zurko & Simon, 1996). Beyond the obvious need to design privacy requirements into a system during the design phase, Zurko and Simon (1996) identify the need to improve applications’ usability, and develop security models and mechanisms for system integration as essential when developing secure applications. The more usable an application is, the easier it will be for users to understand the interactions behind the user interface, and the easier it will be for users to understand security requirements and maintain their own mental model of real security threats to the application.

Adams and Sasse (1999) challenge the assertion that users are inherently careless and therefore responsible for security breaches. They collected 139 questionnaires on password usage, and conducted 30 semi-structured interviews of users in either a technology or construction company. This investigation used Grounded Theory (Strauss & Corbin, 1990) to examine password usage problems and develop a framework of issues affecting user behaviour and to suggest intervention points.

They found that many users circumvented security restrictions to make passwords easy to remember, and had little knowledge of the overall security procedures at work in the organisation (Adams & Sasse, 1999). This led to users constructing their own models of security threats, and these were often wildly inaccurate. When users consider security threats unlikely, or procedures too cumbersome, they often circumvent security measures, which inadvertently leads to a reduction in security. Further findings reinforced a lack of communication between security personnel and users, with each group not understanding the other’s needs.

Adams and Sasse (1999) found four major factors influencing the effective use of passwords: the use of multiple passwords, the password’s content, the perceived compatibility of the security controls with work practices, and the users’ perceptions of organisational security and information sensitivity. The authors make many recommendations for improving password security, including a reduction in passwords, better feedback on password creation and security threats and the use of shared passwords for shared work to create a better sense of shared responsibility. The final suggestion relates specifically for access to group or organisational-specific systems (e.g. a development environment used by an engineering unit) and the tendency of a shared password to create a shared sense of responsibility for a system’s security. This last suggestion is unlikely to be useful in the single-user centric model of service interaction that is at the heart of the ubiquitous computing service architecture explored by this dissertation.

Users interacting with any secure environment must be trained to understand the necessity of security measures, whilst any security design must primarily
acknowledge the main purpose of the system, that is, using an intelligent environment’s services. The study also demonstrated that users equated their ‘user ID’ as another password to be secured, and they fared much better when they had to use only a single password. Biometrics is suggested as a mechanism that further reduces mental overhead, but it has previously been identified as expensive to implement (i.e. high hardware costs) and monitor (Adams & Sasse, 1999). It is suggested that new hardware with biometric devices (e.g. fingerprint scanners that are included on laptops and PDAs) may be useful in the near term, however. Cheaper methods of access control involve users identifying either one of their photos or a sample of their handwriting from a list of decoys.

Architectures should allow the management of users’ interaction within intelligent environments using minimal password entries. Current architectures use mobile devices to interact with intelligent environment services, and these could be used to manage passwords and user access. Users would therefore enter a password to access their handheld device and rely on it to manage their access to individual services. Of course this should be relevant to the information or service being protected, for example, banking services might still require the traditional PIN to be entered, and any additional hardware that is available, e.g. biometric sensors.

Biometric sensors are now being included with many handheld computers, for example thumbprint scanners, and some biometric evaluation can be done with more generic hardware, for example facial recognition using PDA or mobile phone cameras (although these systems are still in their infancy). This could be an effective way of allowing users to confirm who they are to their handheld without requiring them to remember any user names or passwords. This simplification of security for users should provide better security by eliminating the problems of remembering and using multiple alphanumeric passwords.

The user’s mobile device is the least secure aspect of this intelligent environment. Users often lose their devices, fail to use basic security features (e.g. keypad locks, etc.) and rely heavily on social norms (e.g. interaction behaviours) to secure the privacy of their mobile devices (Häkkilä & Chatfield, 2006). The protection provided by social customs may be the more relevant when considering the use of text messages and more direct communication, as it is unlikely to provide sufficient security for devices that can, in effect, act as a proxy for the device’s owner. For example, a personal computer set up to represent a user could be used by a third party to access their email or restricted services, enter restricted areas, or provide information to an environment in a way that violates their privacy preferences.

Mobile devices are increasingly being taken wherever their users go, but many users do not consider what would happen if they lost the device. Identity theft is increasingly a concern in the digital age, and a device that could falsely represent the user in all their normal environments may be a significant security risk indeed. These concerns may cause a rethink of methods of securing a handheld device and ensuring it is still in the possession of the right user. A method of continuous recognition would be...
ideal, for example, voice recognition for voice-activated commands or biometric pheromone recognition. Another method might call for the device to progressively escalate to more secure modes, for example, from activating the keypad lock to eventually deleting the handheld’s contents, as time without contact with the user increases.

2.5.3 Security Applications

This section examines different security applications that could be implemented into a ubiquitous computing environment. Each of the applications described provides a method of addressing a particular objective in application security, for example, secure transport, secure access control and secure service discovery. Pretty Good Privacy (PGP) uses a combination of asymmetric and symmetric encryption keys to provide quick ‘good-enough’ encryption in a one-step encryption channel (Zimmermann, 1995a). Kerberos is a centrally-organised key certificate authority that provides encryption keys to allow secure communication between different system entities (Neuman & Ts'o, 1994). Elvin is a publish-subscribe routing system that forwards messages to users based upon their ‘subscription’ to a message set (Segall, Bill & Arnold, 1997). The advantages and disadvantages of using each of these applications in our intelligent environment architecture are explored below.

2.5.3.1 Pretty Good Privacy

The Pretty Good Privacy (PGP) (Zimmermann, 1995a, 1995b) protocol uses a combination of asymmetric and symmetric encryption (Rivest, Shamir & Adleman, 1978) to speed up the encryption/decryption process. PGP creates a symmetric encryption key and encrypts all information to be transferred. It then encrypts the session key with the intended receiver’s public key and sends both encrypted packages to the receiver (Black, 2000). This process speeds up the encryption/decryption process by only requiring the key be decrypted using an asymmetric key pair. The message is then decrypted using the symmetric session key.

PGP allows users to safely communicate over insecure channels, between two people or between groups of people. PGP can also be used to build ‘chains of trust’ between users, as long as the user knows and trusts someone in the chain (Stajano, 2002, p. 80). This is less important in intelligent environments where users are unlikely to be interacting with users they trust. Such interactions would almost certainly use additional channels outside the intelligent environment, for example, if user A already knows user B, they are likely to communicate verbally (if within line of sight) or via the phone, email or IM.

PGP is effective in providing secure communication channels in the absence of a centralised entity managing key distribution and revocation. This would be particularly useful in intelligent environments where connection to the Internet, or any trusted key-distribution entity, may be unavailable. PGP would therefore be useful as a backup to using a centralised key distribution entity, but it does require that involved parties make their public key available.
to other people in the network. Reuse of the same public key in multiple areas could be a security or privacy risk, allowing intelligent environments (or potentially other users) to recognise the user via previous uses of that public key. This could be avoided through a system using multiple public keys, or by generating a new public key each time the user connects to the intelligent environment. Using a new key would obviously require the re-establishment of trust between the parties.

2.5.3.2 Kerberos

Kerberos is a network authentication protocol developed at MIT in the 1980s. It provides a means of verifying the identities of principals (e.g. a logged-in user or computing device) on an open (unprotected) network (Neuman & Kohl, 1993). This authentication is achieved without relying on the authentication by the host operating system, without basing trust on host addresses or requiring physical security of all the hosts in the network, and under the assumption that packets travelling along the network can be read, modified, and inserted at will (Neuman & Kohl, 1993). This is accomplished by granting users requiring access to entities on the network (including the Kerberos system itself) session keys that are used to encrypt traffic between the two parties.

Kerberos uses an extension of the Needham-Schroeder protocol (Steiner, Neuman & I., 1988) to exchange these session keys with users requesting an interaction ticket from the Kerberos ‘ticket-granting’ service (Neuman & Ts'o, 1994). A ticket and session key is distributed to a client encrypted using the client’s public key, and then this is used to communicate with the service to obtain new interaction keys for different entities in the system. These session keys can then be used to validate the sender’s identity, or to encrypt any communication between the two entities (Neuman & Kohl, 1993), depending on the required security. Kerberos is therefore a distributed authentication service that allows a client running on behalf of a user to prove its identity to a verifier without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal (Neuman & Ts'o, 1994).

Kerberos uses two stages of authentication: a central server to which the user logs on, and a ticket-granting system that gives them access to a particular resource (e.g. a file, a service, etc.) (Anderson, 2001). The Kerberos system uses a login session to provide the user with an electronic token that can be exchanged for a server session key. This session key is a symmetric encryption key used to encrypt and decrypt information exchanged with the server, and thus provides a secure method of exchanging information (Coulouris, Dollimore & Kindberg, 2001). The tokens and session keys both have an expiry time to prevent old session keys being used in masquerading attacks. The use of the session key encryption helps protect users and systems from eavesdropping and message tampering attacks.

The authentication server (or Key Distribution Centre) described here could easily be integrated into an intelligent environment. What is important to consider, though, is how to provide this security without endangering a user's
privacy, or without making the management of this authority too onerous a task. The design decisions for using Kerberos within an intelligent environment surround who controls this authority, and where it would be best served from. A certificate authority within the environment would be less useful for users interacting with multiple environments. An external key distribution centre might be useful for providing keys for users interacting with multiple environments within the neighbourhood, but users would then be reliant on the environment’s Internet connectivity.

Kerberos uses time-stamps (instead of nonces like the Needham-Schroeder Protocol) to allow participants to avoid replay and man-in-the-middle attacks, while the encryption keys used help prevent message changing attacks and maintain confidentiality. Kerberos is susceptible to attack by inducing an error in the network or system’s clock (Anderson, 2001). This can be overcome by using the Network Time Protocol (NTP), which uses authentication of time servers and clock voting in which the clocks vote on the time in a way that makes clock failure and network delays apparent. This would only be effective if a trusted source for the central time were used by the intelligent environment. This would be more effective if any users could independently verify the time with the central source independent of the intelligent environment. This vulnerability may be magnified by the greater risk of tampering with an intelligent environment’s hardware due to its physical accessibility.

Kerberos is particularly vulnerable in its need for a secure password entry point (Neuman & Ts’o, 1994). Users that pick poor or easily-guessed security, or log in to Kerberos using an infected access point (e.g. a terminal with a Trojan house or virus), could be impersonated without the knowledge of other system entities. This suggests that, not only should users receive security training, but mobile or insecure traditional computing devices should also have additional security in place to prevent these vulnerabilities. User centred security is described in section 2.5.2.4, whilst mobile device security is considered in section 5.2.5 and 6.7.2.

2.5.3.3 Elvin

Not all security architectures use encryption and digital verification to secure information exchange. Elvin is a publish-subscribe routing system that allows users to subscribe to content relevant only to them (Segall, Bill & Arnold, 1997). This system separates the distribution of the content from the content producers. This allows the producers of content (described in Elvin as ‘events’), for example a sensor logging the temperature, to send data without a subscription engine. The goal of Elvin is to completely separate the generation and consumption of event notifications, allowing customers to receive information based purely on the attributes of the event (Segall, Bill & Arnold, 1997).

This type of event distribution manager allows new consumers of system events to be added easily to the subscription lists. Consumers can easily alter which events they subscribe to, and the publish-subscribe architecture can easily be scaled to incorporate new systems or environments. Management of
these subscription lists is an obvious method of controlling the distribution of any data within an intelligent environment. However, Elvin does not currently use any form of encryption, and any encryption added to this routing system must scale well and not require encryption/decryption at each point in the delivery chain (Segall, Bill & Arnold, 1997).

Elvin4 controls access to messages through the use of one-way keys (Segall, Bill et al., 2000). Producers may supply a set of raw keys that are transformed by a one-way hash function within the server, prior to matching. To receive a message containing keys, a subscriber must supply one or more keys matching the transformed keys from the producer. The distribution of these keys between the producers and consumers of content is not considered part of Elvin4, and thus any secure system must have an alternative method of distributing these keys between users, for example using shared file systems, directory services or smartcards. A similar method of providing confidentiality over the publish-subscribe architecture using encryption is investigated in (Opyrchal & Prakash, 2001), which uses cluster-based algorithms to provide confidential end-point delivery without a heavy system overhead.

2.5.4 Discussion

This section has described the technical realities of information security within ubiquitous computing environments. Effective security is imperative to maintain user’s privacy within intelligent environments. But the true art in developing security, especially for distributed and potentially untrustworthy systems, is combining effective technical security with adequate data security policies, access control of all resource and information, user training and education.

Each of the security architectures described here is effective under specific circumstances. PGP allows users to securely exchange data with a third party without access to a central server, but does not provide a method to authenticate the sender or receiver. Kerberos provides a centralised key distribution centre to secure communications within an environment, but requires access to a central server and is vulnerable to changes in the server’s clock. Elvin does not explicitly manage information confidentiality, but it does separate the creation of information from its distribution, and scales well for non-encrypted information delivery.

Each of these approaches is likely to be required for some aspect of the intelligent environment architecture. A centralised server for the management of information exchanges within an environment is likely to be useful when a link to such a server is present, but it may make sense for this to be backed up with a PGP protocol for exchanging information in its absence. Information may need to be exchanged within (and between) intelligent environments using the publish/subscribe model. The dissertation investigates how users view privacy within intelligent environments, and develops a secure system to allow the appropriate exchange and utilisation of information within the intelligent environment architecture.
2.6 Summary and Conclusions

There are currently large numbers of intelligent environments that do not provide users with private and secure interaction spaces or the ability to control their information exchanges with the environment. Intelligent environments are currently developed to support specific services, test concepts of privacy and hardware interaction, or to provide test beds for user interactions within ubiquitous computing spaces. This research seeks to identify the privacy, security and interaction requirements that provide users with access to ubiquitous computing services wherever they are.

To develop this interaction infrastructure, this chapter examined existing intelligent environments, risks to user privacy and technical solutions for information security. This was combined with an analysis of methods of interacting with ubiquitous computing systems, the sharing of identity information and fundamental privacy literature to develop an understanding of how users should interact with intelligent environments to maintain their privacy. This understanding was incorporated into the user studies and analysis described in chapter four. The privacy and interaction requirements identified in this chapter were combined with the user study results to develop the requirements for users interacting with multiple intelligent environments, described in chapter five.

The dissertation’s view of the interaction and communication security required within an intelligent environment is developed from the background literature described in section 2.5 and through a review of mechanisms employed in existing intelligent environments. These requirements are integrated into the initial architecture described in section 4.4. The evaluation of the initial architecture and the iterative development of the dissertation’s final architecture further refine these security requirements, and they are described in section 6.2.

The dissertation’s methodological assumptions and research methods are examined in the next chapter to develop a research strategy. These research assumptions will provide grounding for the way this research is conducted, and describe how the researcher views the activities under investigation. Chapter three will also provide a roadmap of the research activities that were undertaken to further develop our understanding of the phenomenon under investigation. The results from this chapter are used to develop the requirements for the user studies in chapter four, and are combined with the user studies’ results in chapter five to develop the interaction and design requirements for the dissertation’s ubiquitous computing infrastructure.
Chapter Three: Methodological Approach

3.1 Introduction

The development of the research approach adopted in the dissertation requires investigation into two areas of study. The first is the deconstruction of the research question to enable the identification of the research assumptions that provide us with a common understanding of how the research topic is to be investigated. The ontological and epistemological assumptions describe the nature of the phenomenon being studied and our understanding of the knowledge under investigation. These provide guidance on the required research methods and help establish a common view for interpreting the research findings. Methodological and ethical assumptions allow us to reflect on the dominant values and goals of our research and to further refine the required research methods.

The second area of concern for this chapter is the development of the research methods and subsequent design that will be used to solve the research question. The Research Methods section describes the methods utilised and evaluates the strengths and weaknesses of each. The individual research activities carried out, and their subsequent impact on each other, are described in detail in the Research Design section (3.6). This chapter ends with an analysis of the appropriateness of using these research methods to solve our research questions.

3.2 Research Questions and Outcomes

In order to achieve the goal of safe and secure ubiquitous computing support, this research examines the privacy and security requirements of intelligent environments. The overarching research question for this thesis is:

**What type of architecture is required to ensure user privacy and information security during service delivery within intelligent environments?**

Intelligent environments have inherent dangers to user security and privacy. Privacy may currently be the biggest concern for intelligent environment developers (Langheinrich, 2001), but what constitutes acceptable privacy is very subjective. User perceptions of privacy vary depending on cultural background, comfort with technology and the perceived benefits of using a particular system. In fact many users are willing to release personal information in exchange for something valuable (Kobsa, 2001). However, what is considered valuable is also subjective.

Information distribution is normally accomplished through wireless transmission, using a particular network design and encryption algorithm. The security design is influenced by the level of security required, e.g. the security required for m-commerce applications will be much greater than that required for the exchange of non-identifiable user information with an intelligent
environment. The use of ultra-secure encryption may be too slow or computationally prohibitive for a given ubiquitous computing system’s components. Many intelligent environments use inexpensive hardware to reduce deployment costs. With these constraints in mind, the dissertation is attempting to identify cost effective (in terms of hardware and computation limitations) security designs that are scalable to multiple intelligent environments.

Beginning with these research goals allows us to evaluate the research sub-questions against the desired research outcomes. The outcomes for this research are evaluated against the following research sub-questions:

- **How do intelligent environments impact on a user’s privacy?**
- **What type of security design is required to ensure the integrity of user data?**
- **How do users interact within an intelligent environment?**
- **What type of design is required to allow users seamless interaction between multiple intelligent environments?**

Table 1 describes the research sub-questions that are used to develop these outcomes.

<table>
<thead>
<tr>
<th>Research Outcomes</th>
<th>Contributing Sub-Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic design strategies to maintain user privacy within an intelligent environment</td>
<td>How do intelligent environments impact on a user’s privacy?</td>
</tr>
<tr>
<td></td>
<td>How do users interact within an intelligent environment?</td>
</tr>
<tr>
<td>Generic design strategies to ensure information security within an intelligent environment</td>
<td>What type of security design is required to ensure the integrity of user data?</td>
</tr>
<tr>
<td></td>
<td>How do users interact within an intelligent environment?</td>
</tr>
<tr>
<td>A model of information flow within an intelligent environment and its effect on user privacy and security</td>
<td>What type of design is required to allow users seamless interaction between multiple intelligent environments?</td>
</tr>
<tr>
<td>Intelligent environment design strategies and a recommended architecture</td>
<td>What type of design is required to allow users seamless interaction between multiple intelligent environments?</td>
</tr>
<tr>
<td></td>
<td>How do users interact within an intelligent environment?</td>
</tr>
</tbody>
</table>

*Table 1: Research Outcomes and Contributing Sub-Questions*

The generic intelligent environment design strategies are examined in chapter four. Results from the user studies in chapter four, along with the design conclusions from chapter two, are developed into specific intelligent environment design requirements in chapter five. The design suggestions form the basis for developing a model of information flow and the infrastructure required for user interaction within intelligent environments. A final architecture is then developed in chapter six with these design requirements and the initial architecture implementations described in chapter four. This scope of the dissertation does not allow for the investigation and
evaluation of user interfaces to share information effectively with users, but the information that is required to be shared is considered.

The ultimate aim of the broad field of research to which this dissertation is intended as a contribution is to move the current intelligent environment state of the art to a place where users can interact with multiple intelligent environments and their services without privacy or security concerns. Evaluation of this goal, however, would require the implementation of numerous intelligent environments with useful services across different physical environments. This is also outside of the scope of the dissertation, but a discussion of these goals occurs in chapter eight.

### 3.3 Research Methodology

A research paradigm typically consists of assumptions about knowledge and how to acquire it. These are associated with the way in which system developers acquire knowledge needed to design the system (epistemological assumptions), and those that relate to their view of the social and technical world (ontological assumptions) (Hirschheim & Klein, 1989). This research examines three paradigms that may be useful in evaluating the required methodological approaches and research outcomes. The selected research paradigms include Positivism, Interpretivism and Critical research. These approaches are summarised in Table 2.

<table>
<thead>
<tr>
<th>Research Paradigm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positivism (Functionalism)</td>
<td>Studies the existence of prior fixed relationships within the phenomenon, which are typically investigated with structured instrumentation. Serves primarily to test theories.</td>
</tr>
<tr>
<td>Interpretivism (Social Relativism)</td>
<td>Attempts to understand the phenomenon through accessing the meanings that participants assign to them.</td>
</tr>
<tr>
<td>Critical</td>
<td>Aim to critique the status quo; studies structural contradictions within social systems to emancipate users from restrictive social conditions.</td>
</tr>
</tbody>
</table>

Table 2: Research Paradigms (adapted from Orlikowski & Baroudi, 1991)

The positivist or functionalist paradigm reflects an objective and regulation position (Iivari, 1991) that considers the existence of fixed relationships between the actors within the system under investigation (Orlikowski & Baroudi, 1991). The interpretive research paradigm "seeks to make sense of human actions by fitting them into a purposeful set of individual aims and a social structure of meanings" (Chua, 1986). It assumes that people create and associate their own subjective and inter-subjective meanings as they interact with the world around them. Interpretivists assume that knowledge should be obtained through the understanding of human and social interaction by which the subjective meaning of the reality is constructed (Walsham, 1995). Due to the social nature of the privacy and the interactions users have with intelligent environments, an interpretivist view of knowledge in this dissertation has been adopted.
Chapter Three: Methodological Approach

Being critical requires the ability to interpret one’s roles and activities in their social context (Stahl, BC & Brookes, 2008). Technology and its intended uses are not value-neutral, but are based on many explicit and implicit value decisions (Adam, 2001). The critical research approach therefore adopts an interpretivist view of knowledge, and seeks to understand a system from the meaning its actors prescribe to it. This approach requires longitudinal studies of the phenomenon at hand, and describes the social context of the system from a historical perspective with a goal of emancipating the actors of the system to allow more effective interaction with the system (Orlikowski & Baroudi, 1991). There are considerable similarities between interpretive and critical research, which explains why some of the principles of the interpretive field research are equally applicable to critical research (Klein & Myers, 1999).

Critical researchers depart from their interpretivist colleagues in that they believe the interpretation of the social world is not enough and that the material conditions of the domination need also to be understood and critiqued (Orlikowski & Baroudi, 1991). While interpretivist researchers aim to “understand and describe the multiple meanings ascribed to an information system and its impacts in a single or different contexts, critical IS researchers go further to expose inherent conflicts and contradictions, hidden structures and mechanisms accountable for these influences” (Cecez-Kecmanovic, 2005). Critical research seeks to develops a theoretical framework not only of ‘what is’, but of what ‘should be’. Critical IS researchers criticize interpretive researchers of accepting the status-quo and seeking merely to understand the social reality instead of ‘acting upon it’ (Cecez-Kecmanovic, 2005).

In order to determine how users perceive the influences on their privacy and security within an intelligent environment, this dissertation must consider the social interaction between the users and the system. While technically implemented, the flow of information, and its effect on users’ privacy and information security, is a socially bound problem. This view of knowledge suggests an interpretivist research paradigm, but the ultimate research goal of emancipating the system’s users from the current dangers of personalised service delivery calls for the critical research paradigm. Only by critically assessing the current interaction methods in intelligent environments can we identify more effective interaction with ubiquitous computing devices.

Stahl (2008) describes critical research as being based upon or inspired by ethics and morality, and the improvement of social reality. In the modern context this describes the emancipation of users through improved access to information and overcoming the digital divide that disempowers users by preventing them from living up to their full potential. To emancipate users from the current impediments to information access, this research must understand the interactions with intelligent environment services that users require. It must then develop an interaction framework that provides access to useful services to enable the empowerment of users without endangering their privacy. The research methods selected will follow these requirements.
3.4 Research Assumptions

The research paradigm adopted has an impact on a range of research assumptions, providing guidance on the research’s ontology, epistemology, methodology and ethics (Burrell & Morgan, 1979). These assumptions cover the view of information within the environment under investigation, how this information can be understood and by what method it should be studied, and finally examine the ethics of the research (in which the benefits that can be derived from the study are made clear). Table 3 describes the research assumptions for the selected Critical approach. This approach reflects the interpretivist groundings in this research’s view of the systems as socially constructed, and the Interpretivistic view of knowledge and the world.

<table>
<thead>
<tr>
<th>Critical Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical and Social Reality (Ontology, Human Rationality and Social Relations)</strong></td>
</tr>
<tr>
<td><strong>Notion of Knowledge (Epistemology and Methodology)</strong></td>
</tr>
<tr>
<td><strong>Knowledge and the Empirical World (Theory and Practice)</strong></td>
</tr>
</tbody>
</table>
Table 3: Research Assumptions relating to an Critical Approach (Orlikowski & Baroudi, 1991)

These research assumptions have been described using Orlikowski & Baroudi’s (1991) view of paradigms in contemporary schools of IS Development. The selected research paradigm was an Critical approach that emphasises the need to understand the social context of the intelligent environment and consider the impact of this context upon the environment’s architecture in order to emancipate users from current designs that pose interaction challenges and inadequate privacy and information security.

3.4.1 Ontological Assumptions

Ontology studies the assumptions made about the phenomenon to be investigated (Iivari & Hirschheim, 1992). Ontological assumptions cover the researchers’ views of information, information systems, human beings, technology and organisations and society. Table 4 describes the ontological assumptions that must be considered for any Information Systems research.

<table>
<thead>
<tr>
<th>Ontology: The assumptions made about the phenomenon being investigated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The view of information/data systems</td>
</tr>
<tr>
<td>The view of human beings</td>
</tr>
<tr>
<td>The view of technology</td>
</tr>
<tr>
<td>The view of organisations and society</td>
</tr>
</tbody>
</table>

Table 4: Ontological Assumptions (adapted from Iivari, 1991)

The dissertation acknowledges that the intelligent environment architecture could be considered a social system, technically implemented. User information within this environment not only describes the user, but the flow of this information helps to define and construct the system. How this information is controlled and utilised will impact on the effectiveness of this new environment.

The dissertation considers humans to be voluntaristic, and thus in control of their actions within an intelligent environment. The view of technology adopted is that technology develops in response to human needs and drives. This is further supported by our ‘nominalism’ assumption of society, in which this environment of user privacy and security does not exist outside the users’ perceptions. This is appropriate given the personal and subjective view of user privacy demonstrated in section 2.4. These assumptions prompt us to consider the importance of user opinion and feedback in interacting with intelligent environments, and to acknowledge this in the research activities.
3.4.2 Epistemological Assumptions

The epistemological assumptions that may be adopted in this research, either positivist or anti-positivist, seek to describe our understanding of the knowledge under investigation (Iivari & Hirschheim, 1992). Positivism states that we seek to ‘explain and predict what happens in the social world by searching for regularities, causal relationships between its constituent elements’ (Burrell & Morgan, 1979). While anti-positivism states that the social world which we are seeking to influence ‘can only be understood from the point of view of the individuals who are directly involved in the activities that are to be studied’ (Burrell & Morgan, 1979). The epistemological assumptions that may be adopted in research are described in Table 5.

<table>
<thead>
<tr>
<th>Positivism</th>
<th>Anti-Positivism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seeks to provide explanation and prediction of the social world.</td>
<td>Seeks to understand the social world by ‘occupying the frame of reference of the participant in action’ (Iivari, 1991).</td>
</tr>
<tr>
<td>The observer is a valid vantage-point for understanding human activities.</td>
<td>The social world can only be understood from the point of view of the participants that are involved in activities.</td>
</tr>
<tr>
<td>Scientific knowledge consists of regularities, causal laws and explanations.</td>
<td>Human interpretation and understanding are constituents of scientific knowledge.</td>
</tr>
</tbody>
</table>

Table 5: Epistemological Assumptions (adapted from Iivari, 1991)

In the developing of our intelligent environment architecture, we must adopt the anti-positivism viewpoint to allow us to create a system to support and improve the actual and perceived privacy and security of users within an intelligent environment. Neo-humanism research (similar to the Critical approach adopted) also uses a positivism approach towards the development of the technology that supports this environment (Hirschheim & Klein, 1989), and the dissertation acknowledges that regularities and causal relationships within the environment must be identified. The dissertation therefore adopts anti-positivism for the analysis of current and required intelligent environment architectures, which supports the critical research paradigm adopted above, but also requires positivistic research activities for the development of the new intelligent environment architecture.

There are contradictory requirements in the dissertation, as an anti-positivism approach is often at odds with the nature of ubiquitous computing research. There are currently no communities that are living and interacting daily with these ubiquitous computing environments. This research therefore will adopt some aspects of positivism, in seeking to identify some causal relationships between users and different aspects of a ubiquitous computing infrastructure. Through this analysis and development of ubiquitous computing infrastructure prototypes, we will then enable research using basic anti-positivism (or user-centric) investigative methods.

These research assumptions acknowledge the importance of identifying user perceptions of privacy and security and the importance of their interactions with their environment. This information will then be used to identify how we can implement these concepts into an architecture that will support the social
interaction of users within an intelligent environment. These assumptions form the basis of the research approaches described in the next section.

### 3.4.3 Methodological Assumptions

Methodological assumptions describe the appropriate choice of research methods. Iivari (1991) identifies three categories of research methods: Constructive, Nomothetic and Ideographic. Table 6 describes the methodological assumptions that may be adopted.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constructive</td>
<td>'The development of various models and frameworks which do not describe any existing reality but rather help to create a new one, and which do not necessarily have any “physical” realisation’ (Iivari, 1991). Constructive research methods include conceptual development and technical development.</td>
</tr>
<tr>
<td>Nomothetic</td>
<td>Characterised by the approach and methods employed in the natural sciences, nomothetic methods focus on ‘testing hypotheses in accordance with the canons of scientific rigor’ (Burrell &amp; Morgan, 1979, p 6). Nomothetic research methods include formal-mathematical analysis, experiments and field studies and surveys.</td>
</tr>
<tr>
<td>Ideographic</td>
<td>Understanding the social world is only possible by gaining 'first hand knowledge of the subject under investigation’ (Burrell &amp; Morgan, 1979, p 6). Stress is placed on knowing the subjects and exploring their background and life history. Ideographic research methods include case studies and action research.</td>
</tr>
</tbody>
</table>

**Table 6: Research Methods (adapted from Iivari, 1991)**

The research assumptions have thus far identified the phenomenon under investigation as a social system, technically implemented. The assumptions normally call for Nomothetic or Idiographic research methods. In order to develop and test an intelligent environment to support this research, some constructive research activities are required. This development will be more related to the development of a better understanding as to what architecture is required, more than it will be used as a tool to improve a user's privacy and information security within a specific existing environment.

This research therefore consists of constructive and nomothetic research activities. Constructive research activities typically consist of conceptual and technical development, and in the dissertation will be concerned with the initial development of intelligent environment architecture and usable prototypes for user testing. Nomothetic research activities typically consist of laboratory and field experiments, field studies and user surveys. The nomothetic research activities will be used to test the developed architecture and to investigate user interaction with the developed intelligent environments. These research activities (of understanding and identifying interaction and privacy requirements) will ultimately support the critical research goal of emancipating users from the current status quo interaction with intelligent environments.
3.4.4 Ethical Assumptions and Ethics of Research

Assumptions surrounding the ethics of research have two aspects. The first aspect is the role of information system science, which can be seen to have three roles: means-end oriented, interpretive and critical. Table 7 describes the ethical assumptions possible for this research.

<table>
<thead>
<tr>
<th>Role of IS Science</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Means-end oriented</td>
<td>Means knowledge for achieving given ends (goals) is provided without considering the legitimacy of the ends.</td>
</tr>
<tr>
<td>Interpretive</td>
<td>Enriches people’s understanding of their actions, and of the production and reproduction of social order (Chua, 1986).</td>
</tr>
<tr>
<td>Critical</td>
<td>Identification and removal of domination and ideological practice (Chua, 1986).</td>
</tr>
</tbody>
</table>

Table 7: Ethical Assumptions (Iivari, 1991)

The dissertation seeks to develop an intelligent environment architecture to maintain and promote user privacy and security. In seeking to develop an architecture, this research is goal-driven, so the actual development uses a means-orientated approach. However, further research is needed to investigate the currently ill-defined architecture requirements. A critical approach is required to consider users’ greater purpose in interacting with ubiquitous computing services, how users interact within an intelligent environment, and how it affects their privacy and security. This approach examines current methods of managing privacy and security, and identifies a more effective interaction framework. These ethical assumptions are in line with Iivari’s (1991) identification that goal-orientated research (as in this case) can be subjected to both means-end orientated and critical analysis.

The second part of ethical assumptions relates to the values of information system research and who benefits from the research. This is important to identify any bias inherent within the research and to frame its results (particularly results of subjective experiments with potentially biased participants). Questions that must be asked to identify the dominant values of the research therefore include:

- Whose values dominate research?
- What values dominate research?
- Whose interests are served by the research?

The dissertation seeks to develop privacy and security aware intelligent environment architecture to promote the use of and potential benefit provided by intelligent environments. The values that dominate this research are those of the intelligent environment’s users (and notably not of the developers or sponsors of these environments). More specifically, the dominant values are the users’ views of their personal privacy and information security. The sponsors’ or developers’ values are considered less important because the aim of the research is to provide an interaction framework that could overcome the major impediment to system usage (i.e. user privacy concerns).
3.5 Research Methods

A mixture of nomothetic and idiographic research methods is adopted to enable the critical goals of this research to be met. The primary methods used are Activity Theory (Cole & Engeström, 1993; Engeström, 1987; Leont’ev, 1978; Vygotsky, 1978), to understand users’ requirements for interacting with ubiquitous computing environments, and Design Science (March & Smith, 1995; Simon, 1981), which provides guidelines for the development of the Intelligent Environment architecture. Critical Heuristics (Ulrich, 1987, 1996, 2008) is also examined to help in the demarcation of the social and technological context of intelligent environments.

The use of Activity Theory and Critical Heuristics in this research seeks to properly delineate the boundaries of the research. This will help develop an understanding as to what in the environment has an impact on the user's privacy and security (and therefore what must be part of the ubiquitous computing infrastructure identified in chapter five). Users’ perceptions of information sharing, privacy and security within intelligent environments are investigated by means of User Surveys and Field Experiments. The intelligent environment architectures developed as part of the Design Science research are evaluated using Field Experiments.

The dissertation's user surveys and field experiments explore the impact that each of the developed intelligent environments have upon user privacy and security. These research activities are conducted and evaluated using Klein and Myers’ seven principles for interpretive field research (Klein & Myers, 1999). These principles highlight the need to place the research findings within the current social and historical context, the need to ensure appropriate abstraction and generalisation analysis is applied to the findings, and the need to identify multiple interpretations of the data from the field studies.

It is important to note that there is a need to study a phenomenon from multiple points of reference from which a more complete picture can be surmised. This is known as triangulation, and is the combination of multiple methodologies in the study of the same phenomenon in order to gain a more accurate representation of a given situation (Jick, 1979). This is also referred to as the ‘principle of multiple interpretations’ (Klein & Myers, 1999). This can be seen in this research primarily in the user studies that investigate the same theory or phenomenon under varying conditions and with different user groups, but also is evident by the numerous complementing research strategies adopted in this investigation.

3.5.1 Activity Theory

Activity theory is a philosophical and cross-disciplinary framework for studying different forms of human practices as development processes, with both individual and social levels interlinked at the same time (Cole & Engeström, 1993; Engeström, 1987). Activity theory is based upon an earlier Soviet-originating cultural-historical research tradition (Leont’ev, 1978; Vygotsky, 1978), which is further grounded in even earlier German philosophical
research traditions (Kuutti, 1995). An activity is comprised of three main parts at an individual level: the subject, the tool and the object (see Figure 5) (Kuutti, 1995). The subject is the actor that interacts with the object using tools to produce a transformation or outcome. The tool assists the user in making the transformation, but ultimately restricts the user to the transformations that the tool is designed for. Interestingly, the object does not necessarily mean a material object; it could also mean an idea or a plan.

![Figure 5: Activity Theory model (Kuutti, 1999)](image)

The greater community (or the activity’s context) has a significant impact on the subject’s use of a given object, and thus this forms an important consideration in the structure of an activity. The social rules of interacting within a community have an impact on the subject’s actions, whilst the interactions of a particular object within the community also develop common guidelines and social imperatives that differ between different contexts. The division of labour refers to implicit and explicit organisation of the community as related to the transformation process of the object into the outcome.

This evaluation of the role of an object in a community compels us to consider the non-technical aspects of its design and consider how it could be better designed for social interaction and immersion within its target community. The Activity Theory model (Figure 5) describes the relationship between the user, available tools and the greater community (including the community’s social norms and division of labour). Activity theory can therefore be used to examine varying levels of the same problem (Kuutti, 1995), allowing the consideration of the application’s greater context, including the usage community and the user’s objectives in the same integrated framework. This evaluation of social context also provides us with a means to evaluate dynamic systems and tailor development to users’ interaction objectives and social context, and not just to a particular service or interaction requirement.

Activity theory’s main strengths are its evaluation and acknowledgement of the social context and dynamic nature of the activity. But its failings are a lack of guidance for specific development and analysis of the activity’s composite parts. This weakness essentially demands that this research method be used in conjunction with more traditional constructive research methods like conceptual and technical development techniques, and evaluative techniques like case studies and field experiments.
Activity Theory focuses research on the interrelated nature of the environment and its inhabitants. It is important to consider the interaction subjects (the users), their community and their objectives (the desired outcome of the user’s interaction) in interacting with the tool under investigation. Study of the social rules and regular methods of interaction (the division of labour) is essential to understand their impacts on the environment, the actors and their objectives. The actors and their objectives must be understood before we can develop the tools that allow interaction within the digital community that resides across the user’s physical environments.

The activity under investigation is the interaction with intelligent environments to receive a particular service or information on an environmental entity (e.g. another user). The subjects in this research are users that are interacting with our developed intelligent environments and provide feedback on the tasks that occur within (e.g. information sharing in ubiquitous computing environments). The objects are the services that the users want to access. This could be simply a request for more information from another user. The transformation is the process for delivering a service, with the outcome being the service information (or goods etc.) or the results of any information request (whether or not it was successful). The division of labour refers to implicit and explicit organisation of the community as related to the transformation process of the object into the outcome. In this example, the division of labour could include the use of third-party identity management or service providers that form part of the transformation process. These are also included as an important part of modelling the activity.

The tool in the dissertation’s research refers to the user’s interface into an intelligent environment, and any service interface that may be available. These computing interfaces provide the means to acquire new information or services and are currently very environmentally specific. Improving the general tools available to the users will go a long way towards enabling the mass utilisation of these services and allowing effective information sharing. The dissertation examines the integration of the tools and their ability to effectively manipulate the given objects (and objectives) within the current community. On the other hand, the development of the community to better support intelligent environment services and user interaction is essential.

The community in this context refers to the current physical and technical environments from which users interact with ubiquitous computing services. This includes the social community’s perceptions of ubiquitous computing technologies (in particular their privacy and security), or the Rules, and the structures available in the community to promote secure information sharing, or the division of labour. Understanding these users’ perceptions allows us to design culturally appropriate tools for information sharing without rendering their use unpalatable due to privacy concerns. The deconstruction of required environmental entities for managing identity and information exchanges further improves the users’ ability to meet their objectives in an intelligent environment (e.g. sharing information in a secure and private manner to receive a service).
3.5.1.1 Strengths and Weaknesses

Among the strengths of Activity Theory is its holistic approach to the investigation of a particular phenomenon. Ubiquitous computing environments, whilst being the main infrastructure for service delivery, are not the primary phenomenon under investigation. The dissertation’s research addresses the desire of users to interact with each other, and with services, in a natural way across their daily lives. The services that are desired will vary between users, physical environments and social settings. The dissertation is therefore focused on how this interaction should take place, and what infrastructure is required to allow this service delivery in a manner consistent with users’ desires and interaction requirements.

The use of activity theory highlights important areas of concern that this research must examine. Obviously the architecture developed will address multiple areas of the activity, from the tools that users utilise to interact with the intelligent environments, to the external entities necessary for these interactions in the greater environment. We must also consider how the required architecture could affect other areas that have an impact on the interaction with ubiquitous computing environments. The social rules and norms that currently govern users’ interactions with these technologies will evolve as their abilities improve. This will in turn influence the community and ultimately redefine how users and the greater community feel about ubiquitous computing and the forms of information sharing that go with it.

It is important to note the goals of this research in developing a private and secure intelligent environment architecture. There will be the need to evaluate and understand the community, social norms and rules governing the stated object (and users’ objectives), but this research necessarily focuses on the tools and ‘division of labour’ required to achieve the types of transformation required. This focus is to the detriment of advice on the development of the community, social norms and subject’s perceptions of information sharing and ubiquitous computing technologies. To focus on these goals would be outside the scope of this research, as it would require a large user base and the extended implementation of multiple intelligent environments in real-world locations. The lack of useful and engaging intelligent environments ready for widespread adoptions makes these goals unrealistic. In addition the potential variation of communities and social norms, between different user groups or countries, means that there is more value in producing an architecture that encompasses these differences than providing specific advice on changes required in any given community or social behaviours, something that is difficult at best to achieve in any case.

While Activity Theory’s main strengths are its acknowledgement and evaluation of the social context and dynamic interrelated nature of the phenomenon under investigation, its failing is the lack of guidance for specific analysis of its composite parts. This weakness essentially demands that this research method be used in conjunction with more traditional evaluative and constructivistic research methods. To supplement this weakness, this research will adopt field studies (e.g. surveys) and experiments (e.g. field and laboratory experiments) to help investigate the community and users’
perceptions of information sharing in line with our nomothetic research approach. Activity Theory will also be supported with Design Science methods to support the construction of the appropriate tools to support users’ activities in these environments.

3.5.1.2 Summary
Activity Theory will be used in this research to develop a complete picture of the influences of users’ information sharing and service interaction within ubiquitous computing environments. This theory prompts us to consider the impact of the users, social norms, community and existing and future divisions of labour that might impact users’ interactions with these environments. This theory will be combined with Design Science, Field Experiments and Laboratory Experiments to improve our understanding of these influences and in the construction of tools to help users meet their interaction goals.

3.5.2 Critical Heuristics
Critical Heuristics is an approach to systems thinking and practical design that seeks to support researchers in delineating their research problems based upon their environmental, philosophical (value judgements) and technological (system) context (Ulrich, 1987). Critical heuristics not only describes the value judgements (or normative premises) that are inherent in the practical position under study (i.e. the action or design model) but also their normative implications in the context of their application (Ulrich, 1987). This research approach is used in conjunction with more traditional design methods and is used to provide the researcher with a greater understanding of what is (and what is not) part of the system under investigation.

The value judgements applied during the application of critical heuristics are in the form of either whole-system or boundary judgements. Whole-system judgements relate to what lies within the scope of the research effort and what lies outside it. Boundary judgements are those judgements by means of which we define or question the boundaries of a reference system. In this context the reference system means “the context that matters when it comes to assessing the merits and defects of the proposition” (Ulrich, 2000). Boundary judgements will be developed for this research in an attempt to identify what aspects of an intelligent environment architecture impact on user privacy, and in a more general sense what structures are required in a ubiquitous computing infrastructure to support user privacy and information security.

Critical heuristics calls for the evaluation of the boundary judgements, particularly for critical purposes. The process of boundary critique focuses on the underlying assumptions of the system design and the identification of any other influences that may impact the design of the action or design model under investigation. Indeed, any aspects of a system that are not understood must be considered part of the system under study and not part of the ‘greater environment’ that is considered outside of the study (Ulrich, 1987). In this research the users of the intelligent environments must be part of the
evaluation, as their perceptions of privacy and security will have a crucial impact on the success or failure of the intelligent environment architecture.

Critical heuristics research is ideal for ubiquitous computing systems development due to the extensive influence that contextual factors have upon their use and effectiveness, and critical heuristics’ strength in classifying and evaluating the relevance of these contextual influences (Ulrich, 2008). Further justification for the suitability of this method lies in its design to identify the ‘ideal solution’ for the phenomenon under investigation (Ulrich, 1987). This is reflected in Table 8 (in the next section) that compares the current state (‘is’) with the ideal state (‘ought to’). This research will therefore develop the ideal architecture for effective service interaction and adequate user privacy and security, which is consistent with the critical paradigm selected in section 3.3.

### 3.5.2.1 Boundary Justification Critique

This section examines the logical boundaries of the dissertation’s research activities, specifically by comparing the boundaries of current intelligent environments development (the ‘is’ column) with the boundaries in the ideal case (the ‘ought to’ column). The following table details the responses to the 12 boundary checklist questions whose answers ‘inevitably flow as normative premises into any concrete system design’ (Ulrich, 1987).

<table>
<thead>
<tr>
<th>Mode</th>
<th>‘Ought to’</th>
<th>‘Is’</th>
<th>Design Requirements: Critique ‘Is’ against ‘Ought to’</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client</strong></td>
<td>Intelligent Environment Users</td>
<td>Intelligent Environment Developers, Designers</td>
<td>Ideal case should seek to support use interaction (privacy and security requirements) as these fundamentally impact users’ willingness to interact with the system.</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Interaction within multiple intelligent environments for user interaction and services delivery</td>
<td>Interaction with intelligent environment users or the delivery of particular services</td>
<td>Must focus on the development of multiple intelligent environments and the impact this has upon user privacy (as well as the technical evaluation of security and interaction protocols).</td>
</tr>
<tr>
<td><strong>Measure of Improvement</strong></td>
<td>Ability to interact with environment privately and securely</td>
<td>Ability of users to interact with service or other users</td>
<td>Changes to user privacy and realising the ability to interact privately with multiple intelligent environments simultaneously and with different identities or personae.</td>
</tr>
<tr>
<td><strong>Decision-maker</strong></td>
<td>User of intelligent environment and services</td>
<td>Designer of intelligent environment and service</td>
<td>Moves from the satisfaction of the designer with the service delivery, to the satisfaction of the user’s interaction with the environment and services.</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>Control over information to allow evaluation of the need for identity authentication and the provision of identity information</td>
<td>Intelligent environment for analysis and evaluation of technical interaction (and information flows etc.)</td>
<td>Need to investigate users’ perceptions of interaction within intelligent environments, especially relating to personal information, privacy and information security concerns.</td>
</tr>
<tr>
<td><strong>Decision environment</strong></td>
<td>Users’ interactions with multiple intelligent</td>
<td>Users interactions within one intelligent</td>
<td>Only a holistic view of user interaction with multiple intelligent environments could hope to develop a scalable, private and</td>
</tr>
</tbody>
</table>
Chapter Three: Methodological Approach

The dissertation therefore must consider the global environmental infrastructure as well as the intelligent environment's architecture. Sources of Knowledge

**Professional**
- Users, Security Designers
- Ubiquitous Computing System Designer, Security Designers

**Expertise**
- Perceptions of Privacy, Information Security
- Technical interaction capabilities, Information Security

**Guarantee**
- Privacy: consensus amongst users, user participation, political support (privacy groups)
- Security: consensus amongst experts, lack of negative usage feedback
- Technical: consensus amongst experts, acceptance of interface amongst users
- Security: consensus amongst experts, lack of negative usage feedback

**Sources of Legitimacy**

**Witness**
- Technical Security and (Social) Privacy Researchers
- Technical Security and Ubiquitous Computing Researchers

**Emancipation**
- Ability to interact with multiple intelligent environments (and its services) privately, securely and using the same identity options that are available in the real world; overcoming natural resistance to ubiquitous computing systems
- Providing the ability to deliver context-aware services to users via ubiquitous computing systems

**Worldview**
- Effective (private and secure) interaction across multiple intelligent environments
- Effective (private and secure) interaction with a single intelligent environment

**Sources of Knowledge**

**Sources of Legitimacy**

**Witness**
- Technical Security and (Social) Privacy Researchers
- Technical Security and Ubiquitous Computing Researchers

**Emancipation**
- Ability to interact with multiple intelligent environments (and its services) privately, securely and using the same identity options that are available in the real world; overcoming natural resistance to ubiquitous computing systems
- Providing the ability to deliver context-aware services to users via ubiquitous computing systems

**Worldview**
- Effective (private and secure) interaction across multiple intelligent environments
- Effective (private and secure) interaction with a single intelligent environment

**Sources of Legitimacy**

**Witness**
- Technical Security and (Social) Privacy Researchers
- Technical Security and Ubiquitous Computing Researchers

**Emancipation**
- Ability to interact with multiple intelligent environments (and its services) privately, securely and using the same identity options that are available in the real world; overcoming natural resistance to ubiquitous computing systems
- Providing the ability to deliver context-aware services to users via ubiquitous computing systems

**Worldview**
- Effective (private and secure) interaction across multiple intelligent environments
- Effective (private and secure) interaction with a single intelligent environment

**Table 8: Boundary Justification Critique (Ulrich, 1996, p. 44; cited in Ulrich, 2008)**

The obvious conclusion that can be drawn from this evaluation is the need to understand not only the user’s place within the intelligent environment architecture, but also the impact of the greater environmental infrastructure on the user’s interaction motivations. This critique highlights the importance of not only recreating the same interactions users have in the real world, but also the need for their involvement (and the recognition of their interaction goals) from the beginning of the design process. Instead of developing a single (stand-alone) intelligent environment, the dissertation must also consider the design goals of scalability, global infrastructure support structures and interaction with multiple environments.
3.5.2.2 Summary

The evaluation of the intelligent environments’ justification boundary is a necessary aspect of the dissertation. The initial work presented in chapter four attempts to understand intelligent environment and service interaction problems, and seeks to identify heuristical design conclusions about the intelligent environment interaction requirements of users that lead to better privacy outcomes. Conclusions from these research activities (sections 3.6.1-4) form the basis of the dissertation’s recommended ubiquitous computing infrastructure and the intelligent environment’s design suggestions described in chapter five.

3.5.3 Design Science

An extension of the ‘Natural Sciences’, design science is concerned with ‘devising artefacts to attain goals’ (Simon, 1981). Whilst the natural sciences seek to describe reality, design science seeks to provide a technological solution to a problem in a given environment (March & Smith, 1995). In this paradigm, knowledge and understanding of the problem domain and its solutions are achieved by the building and evaluation of the designed artefact (Hevner et al., 2004). In this research the construction and evaluation of intelligent environments are used to inform on the required design for a ubiquitous computing infrastructure that allows users private and secure interaction with their environment.

The design science paradigm seeks to extend the boundaries of human and organisational capabilities by creating new and innovative artefacts (Hevner et al., 2004). As technical knowledge grows, it is applied to new applications, areas that were not previously believed to be amenable to IT support (Markus, Majchrzak & Gasser, 2002, p.180). This is the case in this research, as it studies privacy and methods of interacting within existing environments, using new computing techniques and systems (i.e. ubiquitous computing). The evaluation of the requirements of this environment, coupled with the use of Activity Theory in investigating users’ desired activities, will help broaden our understanding of what users want from this interaction space, and allow a more complete picture of the activities and interaction requirements to be supported by the architecture.

The use of the design science research approach has a clear set of guidelines to use when developing a research project. These research guidelines were developed by Hevner, March et al. (2004) to assist researchers, reviewers, editors and readers to understand the requirements of design science research. Whilst Klein and Myers’ (1999) warning against the mandatory or rote use of design guidelines is acknowledged, these guidelines offer a systematic way of evaluating seven different aspects of design research. The guidelines (considered in depth for this research in section 3.5.3.1) examine:

- Design as an artefact
- Problem Relevance
- Design Evaluation
- Research Contributions
Chapter Three: Methodological Approach

- Research Rigor
- Design as a Search Process
- Communication of Research Results

Design science research in IS addresses problems which are considered to be 'wicked problems' (Brooks, 1987, 1996; Rittel & Webber, 1984). These problems are characterised by:

- unstable requirements and constraints based upon ill-defined environmental contexts
- complex interactions among sub-components of the problem and its solution
- inherent flexibility to change design processes as well as design artefacts
- a critical dependence upon human cognitive and social abilities to produce effective solutions

A significant issue with researching these ‘wicked’ problems is their instability. People’s interaction requirements and expectations can change rapidly as they become accustomed to new interaction methods and system capabilities. Results from this research must acknowledge the rapidly changing nature of the phenomenon under investigation and allow for a change in user interaction and privacy requirements. Design science varies from the natural sciences that seek to find a ‘truth’ or absolute correct solution to a given problem (Hevner et al., 2004). Design science seeks a ‘good enough’ solution that can be more readily reached for the complex and unstable wicked problems like the one addressed by this dissertation.

The dangers of design science research are an overemphasis on the design of technology and a failure to maintain an adequate theory base, potentially resulting in well-designed artefacts that are useless in their contextual setting (Hevner et al., 2004). To be effective, any research developing technological artefacts must consider not only the technical issues at hand, but must also identify the impact of users’ perceptions of the artefact on its use and account for the varied nature of the environments in which it may be deployed. Some behavioural science research activities (e.g. Field Studies) should therefore be considered to investigate these factors that may have a significant impact on the artefact’s success.

This research will utilise the design science paradigm in the investigation of the social and technical constraints on the design of privacy- and security-aware intelligent environments. This development will be driven by the analysis of current and potential intelligent environments, utilising surveys and field and laboratory experiments, based upon the overall Activity Theory research approach. In this paradigm, knowledge and understanding of the problem domain and its solutions are achieved by the building and evaluation of the designed artefact (Hevner et al., 2004). This is the case in this research, as it studies privacy and methods of interacting within existing environments, using new computing techniques and systems (i.e. ubiquitous computing). The evaluation of the requirements of this environment, coupled with the use of Activity Theory in investigating users’ desired activities, will
help broaden our understanding of what users want from this interaction space, and allow a more complete picture of the activities and interaction requirements to be supported by the architecture.

3.5.3.1 Research Guidelines

The following section describes the design decisions formed through an analysis of the seven design science research guidelines (Hevner et al., 2004).

Guideline 1: Design as an artefact

The dissertation develops a scalable intelligent environment architecture that protects users’ identity whilst allowing the provision of secured services. The development of this architecture allows us to examine the greater problem of designing a ubiquitous computing infrastructure that is usable and useful to both users and service deliverers. The development of each architecture (or the research’s artefact) allows the evaluation of both the technical abilities of the artefact and the users’ interaction requirements in this space. The research design for the development of this architecture is described in sections 3.6.3 and 3.6.6, and the architecture is described in chapter six.

Guideline 2: Problem Relevance

Ubiquitous computing environments use invisible information collection and transfer that make users nervous, and dramatically affect users’ perceptions of these new systems (Langheinrich, 2001). This concern in the age of identity theft and big brother surveillance has the ability to scuttle the usefulness of intelligent environments to provide users with personalised, contextually aware services. The goal of this research is to provide a secure and private interaction architecture that allows users to take advantage of these services without having to risk privacy breaches or information insecurity. The relevance of developing a unifying intelligent environment architecture is described in more detail in section 2.2.

Guideline 3: Design Evaluation

The evaluation of this design will occur on two levels. The first describes technical flaws in the architecture that would allow a breach of security, potentially damaging users’ privacy. The second examines users’ perceptions of privacy and the expected levels of anonymity within these systems. The architecture developed in the dissertation is therefore evaluated by a theoretical evaluation of its technical integrity and via field studies with users evaluating its ability to preserve privacy in a useful and usable manner.

The dissertation does not evaluate the impact that intelligent environments, or the ubiquitous computing infrastructure, have upon their users’ lives. To understand this problem, a wide-scale implementation involving a large number of users across a significant number of their everyday environments would be required. This study would be useful in further examining users’ interaction and privacy requirements within intelligent environments, but given its scale and the unavailability of resources for these research activities, this evaluation will necessarily be left for further studies.
Guideline 4: Research Contributions

The design science contributions of this research are the identification of the requirements for a ubiquitous computing infrastructure and the development of a secure privacy-aware intelligent environment architecture. This architecture is the first identified to consider privacy and information security before the development of the intelligent environment, and is therefore in a unique position to influence the development of all intelligent environments. The development of a ubiquitous computing infrastructure has great potential to change the way we interact with our everyday environments, and can provide interesting support services for local communities (e.g. provide virtual community interaction spaces or local history and directions).

Guideline 5: Research Rigor

Artefacts designed using the design science approach must be rigorously defined, formally represented, coherent and internally consistent (Hevner et al., 2004). This is especially the case here if we are to develop a reference infrastructure (or architecture) for the development of all intelligent environments. Chapter four defines the problem domain and required attributes of these systems. The level of security within these systems is evaluated using existing literature on security design. User privacy is examined through the evaluation of the architecture (in part using Activity Theory) to describe interaction activities that the artefact must support, and through field studies, to allow users a chance to interact with these systems in a controlled environment. Each of these evaluation techniques is described in detail below.

Guideline 6: Design as a Search Process

Design science is inherently iterative, and the search for the correct solution to our problem relies on the generate design/test cycle of development (Simon, 1981). The solutions developed in this research seek to understand the requirements for a ubiquitous computing infrastructure through user studies and field experiments. The user studies examine users’ perceptions of sharing information within ubiquitous computing environments, providing a better understanding of the problem space. Field studies examine users’ interaction with the developed intelligent environment architecture in real world settings. An iterative development process is used to allow design environments based upon the identified technical and user requirements, and to allow adequate user testing to refine this design.

Design guidelines for this architecture were developed by reviewing relevant privacy and security literature and by examining the approaches of existing intelligent environments. These guidelines were then used to develop an initial architecture, and this was in turn evaluated through users’ tests and comparisons with existing systems. This iterative design process is further described in section 3.6. It must be recognised that this architecture still requires a longitudinal evaluation in a real-world setting, something that is not possible in the dissertation given the complexity (and length) of this evaluation and the resources that would be required.
Guideline 7: Communication of Research

This guideline describes the need to effectively communicate the dissertation's findings to all interested parties, including those with either a technical or managerial focus (Hevner et al., 2004). The results of this research are interesting for the developer of an intelligent environment, as they guide the development of a private and secure system. The results are also of interest to researchers examining the concept of privacy and users’ perceptions on ubiquitous computing. It is also hoped that the developed architecture will promote further research into new forms of digital communities supported by ubiquitous computing systems.

A number of outcomes will result from this research. The primary outcome is the characterisation of the required attributes of a ubiquitous computing infrastructure that could provide context aware and locally relevant services to users in the environment. It is important that these findings be well grounded in both existing research and in our user studies of the perceptions of information sharing within ubiquitous computing. These topics are explored in chapter two (background literature) and chapter four (user studies), while the overall design requirements are considered in chapter five.

The second outcome is the architecture that will allow a private and secure interconnected, distributed ubiquitous computing infrastructure. This architecture is implementation independent, and describes design goals that were identified as important to users’ privacy in these environments. This will allow future developers and ubiquitous computing researchers to develop private and secure intelligent environments, and allows us to consider what could be the overall impact of using these new technologies. The intelligent environment architecture is defined and evaluated in chapter six.

The third set of outcomes is the prototypes developed to provide proof of concept interactions to users for the field studies testing initial architecture designs. As these prototypes were only ever intended for use in our field studies, much of the already proven security mechanisms were abstracted to allow for more rapid development. The abstractions of any part of the prototype designs are documented in their particular sections. These abstractions have no impact on the overall validity of our results, as these field studies were examining users’ interactions and perceptions of the represented information exchanges between the user and the environment.

3.5.3.2 Strengths and Weaknesses

The development of a private and secure architecture for interacting with a ubiquitous computing infrastructure fits well with the description of a ‘wicked problem’. These environments contain countless dependent and independent entities that must interact with a wide range of different contexts and users. Furthermore, the importance and subjectivity of a user’s privacy perceptions, and the inherent need for flexibility in the solution, make these designs much more difficult. Solutions therefore need to include user controls to allow different types of interaction and service usage, and should allow at least
some dependency on their users’ cognitive and social abilities. This suggests that the design science paradigm is suitable to address our research problem.

The dangers of design science research is an overemphasis on the design of technology and a failure to maintain an adequate theory base, potentially resulting in well-designed artefacts that are useless in their contextual setting (Hevner et al., 2004). This research clearly needs to address not only the technical issues at hand, but also to identify the impact of users’ perceptions and must account for the varied nature of the environments in which it may be deployed. Some behavioural science research activities (e.g. Field Studies) will therefore be required to provide additional guidance on users’ perceived issues with interacting with a ubiquitous computing infrastructure and to ensure the solution is adaptable to any given context.

3.5.3.3 Summary

The use of design science in this research is appropriate, but this must be combined with behavioural science activities to provide additional guidance on the required interaction within the ubiquitous computing infrastructure. These opposing views will allow effective identification of the technical (positivistic) and user-perceived (anti-positivistic) requirements of our architecture. The presentation of the design science guidelines allows us to more thoroughly describe our research project and reinforces the understanding of the required research activities.

3.5.4 Field Studies

Field Studies are experiments in which a particular artefact or phenomenon is studied in a natural environment. Field studies are further comprised of natural experiments and field experiments. A laboratory experiment describes an experiment not grounded in a natural environment.

A natural experiment brings an experimental interpretation to an event or process that has already taken place or that will take place in the future without any proactive effort by the researcher (Järvinen, 2004). Field experiments create an event or process to study, but the study remains in the field (i.e. the natural setting of the phenomenon under study). This localisation provides the study’s participants with more context and meaning, providing a more realistic experience, and allows the researcher to observe the interaction in its natural setting. These make field experiments a more valuable research tool (McMurray, Pace & Scott, 2004), at the cost of less control over the study.

Stone (1978, p. 118) identifies the following attributes of laboratory experiments: the research takes place in an artificial setting; the researcher assigns subjects to treatment and control conditions; the researcher manipulates one or more independent variables and assesses their impact on the dependent variables; and the experimenter has control over virtually all the independent and intervening variables that affect the dependent variables. The major criticism of laboratory experiments relates to external validity. This gives rise to the complaint that laboratory experiments lack
realism, or that there is a lack of correspondence between natural events and events in the laboratory (Stone, 1978, p. 120).

An important aspect of Field Studies is their internal and external validity. Internal validity refers to the validity of a researcher’s conclusions that the relationship between the independent and dependent variables is causal or that the absence of such a relationship implies a lack of causality. External validity is the degree to which the causal relationships observed can be generalised to other populations, settings and times (Cook & Campbell, 1979). Cook and Campbell (1979) suggest that to improve external validity researchers must choose a target setting and population about which they wish to generalise and draw a representative sample for that target. They also suggest that external validity can be enhanced by replication both within a study and across studies, and by using triangulation by approaching the same problem using different experiments and experimental instruments.

Any experimental design must recognise the tension between the need for the results to be generalisable with the need for the results to be interpretable, or the tension between the need to control external variables (laboratory experiments) with the need for the study to take place in its natural setting (field experiments). In general the more natural the experimental situation, the more generalisable the findings; the greater the experimental control, the more interpretable the findings (Järvinen, 2004).

The nomothetic methodology assumptions held by this research call for the investigation of the phenomenon using laboratory experiments, field studies and surveys. In this instance field studies would refer to case study investigations of users interacting with existing intelligent environments in a given environment. Unfortunately these environments have yet to be integrated into users’ everyday environments, and such a study site is not accessible. This research therefore uses a mix of user surveys (described below) and field studies.

The dissertation’s user studies require high external validity, so the results can be related to other populations and produce a statement of the privacy and security requirements for users interacting with intelligent environments. To accomplish this we must choose a target setting and population about which we wish to generalise and draw a representative sample for that target. To further increase this external validity, we must replicate important aspects of our studies that we wish to draw conclusions from both within a study and across studies. This is reflected in the choice of the representative population for the experiments, including early adopters of technology that are likely to utilise ubiquitous computing services to support activities in their daily lives, and in the replication of similar questions within different studies to provide triangulation and validation of the experiments’ findings.

The dissertation examines users’ perceptions of information sharing and interaction with new forms of ubiquitous computing environments. In this situation there are very few controllable influences on the users’ perceptions when accessing Intelligent Environment’s services. More important here is how the users will relate to these environments in their natural setting. This
research adopts field experiments (over laboratory experiments) to ensure a high external validity in our findings. This evaluation in turn is fed back into the development process, allowing users to influence the design by refining the objects and tools entities described in the Activity Theory section (3.5.1). The field experiments planned for this research are described in sections 3.6.2, 3.6.4 and 3.6.7.

3.5.5 Survey Research

Survey research involves gathering information for scientific purposes from a sample of a population using standardised instruments or protocols (Järvinen, 2004). This information gathering could utilise a number of different techniques, such as the use of questionnaires, field interviews or direct observations of users or working systems. Survey research has three distinctive characteristics. Firstly it is designed to produce quantitative descriptions of some aspects of the study population (although qualitative data is often also collected). The second characteristic is that the principal means of collecting information is through asking people structured, predefined questions. And finally, information is generally collected about only a fraction of the study population – a sample – and is collected in such a way as to be able to generalise findings to the population.

The use of ‘structured, predefined questions’ does not preclude open questions that are designed to gather general and perhaps unknown information about a general topic. Structured questions provide all possible responses to the responder, while open questions are formulated so that a respondent can give short or long responses using their own terms (Järvinen, 2004). When using this approach the researcher poses structured questions when they already have a hypothesis on the likely responses to a question.

Randomisation and the assumptions of normal distribution are difficult to achieve in field research (Cunningham, 1997; McMurray, Pace & Scott, 2004). A large percentage of organisational researchers use convenience samples as opposed to random samples, and reviews of many samples indicate that distributions are not normal. It is realistic to expect that most studies will therefore be unrepresentative, and it is important to consider the representativeness of the sample (Cunningham, 1997; McMurray, Pace & Scott, 2004). Validation of the sample’s representativeness can include five different methods: i) checking the results with experts in the field setting, ii) increasing the number of instances and encouraging other perspectives, iii) carrying out other studies in similar settings, iv) looking purposefully for contradicting instances and v) sorting the instances to look for differences (McMurray, Pace & Scott, 2004). This is especially important when using students in laboratory experiments and when using volunteers, as they tend to be in a different group from non-responders. Responders tend to be brighter, better workers, more motivated and more highly educated about a topic.

The strengths of using field research methods are their ability to provide qualitative user evaluations about the phenomenon under examination, in this case the impact of privacy and security, and that they provide the means to
generalise these results to the greater population. This generalisation is based upon the external validity of the survey method and the representativeness of the sample population used in the test. A research activity is said to lack external validity when its results cannot be generalised to groups other than those that participated in the original survey.

The selection or availability of a representative sample for a given field study is an obvious weakness of these methods. Population samples must include a cross section of the likely or known users for a given system, and where possible should seek to include users less likely to volunteer for a survey or field study. Survey questions posed to participants should also be evaluated for clarity, usefulness and ambiguity, using the guidelines set out in (McMurray, Pace et al. 2004).

This research utilises user surveys to gather information on perceptions of information sharing, privacy and other aspects of interaction with intelligent environments (e.g. use of a mobile device). This allows the gathering of information from a larger audience than when using field or laboratory experiments alone, and allows the introduction of exploratory questions (using short answer or open-ended questions) early in the research to generate new avenues of study. A concern with conducting these surveys within a university setting is the potential to over represent a section of the population (e.g. students) in the results, even when the selection of this particular user group may be appropriate.

To address this, care is taken to consider the representativeness of our research population in any user surveys, especially in the analysis of the generalisability of any research results. Research results are considered in light of any potential over representation, and the dissertation’s literature review and additional research activities (e.g. additional studies with wider audiences) will seek to identify contradicting results. With these caveats in mind, the use of university personnel and students is treated in this dissertation as being a reasonable proxy for a random sample of early adopters. The external validity of the results is accordingly limited by the unproven nature of that assumption, and limited to early adopters.

Intelligent environments provide an interesting case due to the lack of real-world applications currently deployed in potential users’ environments. Population samples are therefore more likely to focus on generic skills and characteristics and the willingness to adapt to new technologies. These restrictions must be acknowledged in the research design, and subsequently these concerns are raised when discussing the design of any user studies within this research. User surveys are used to investigate users’ perceptions of privacy and security within intelligent environments. This investigation also examines users’ use of mobile phones and influences on users’ willingness to share information with third parties within these environments. This research activity is described in sections 3.6.1 and 4.2.
3.6 Research Design

Due to the emerging nature of ubiquitous computing development, existing research in this area tends to follow a design science approach using clearly defined requirements (e.g. create a communication protocol for simple wireless beacons, or develop an environment that can provide a specific service to the user’s handheld computer). These environments are usually then tested by other computer science experts (including developers and students), and further developmental iterations are carried out. In this development we were initially unclear as to the users’ perceptions of privacy and how they would want to interact with services in their natural environments. The design science approach in this case was augmented with activity theory to add more structure in the search for users’ privacy and interaction requirements within our intelligent environment.

This section describes the research activities that were carried out to solve the research questions set out in section 3.2. These activities investigate the socially complex interaction requirements for intelligent environments and seek to develop a private and secure technical design to meet these needs. The seven planned activities can therefore be separated into constructive and nomothetic research activities. Brief descriptions of these research activities are provided in Table 9, their relationships are described graphically in Figure 6, and they are described in more detail below.

<table>
<thead>
<tr>
<th>Research Activity</th>
<th>Description/Research Methods Adopted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 User Perceptions of Information Sharing</td>
<td>Investigation of Users’ Perceptions of information sharing within ubiquitous computing environments. Use of Survey Research (Questionnaires)</td>
</tr>
<tr>
<td>2 Personalisation in Intelligent Environments</td>
<td>Evaluation of effect of context-awareness and personalisation on users’ digital identity management. Use of Activity Theory and Design Science</td>
</tr>
<tr>
<td>3 Initial Intelligent Environment Architecture Development</td>
<td>Implementation of an intelligent environment using a new privacy-aware architecture. Use of Design Science and Activity Theory</td>
</tr>
<tr>
<td>4 User Study of Initial Intelligent Environment Architecture</td>
<td>Evaluation of user interactions within initial intelligent environment, in particular examining the effect of the intelligent environment on user privacy and information security. Use of Field Studies</td>
</tr>
<tr>
<td>5 Development of Ubiquitous Computing Infrastructure Requirements</td>
<td>Evaluation of technical and user interaction design requirements for a private and secure ubiquitous computing infrastructure. Use of Activity Theory, Critical Heuristics and Design Science</td>
</tr>
<tr>
<td>6 Development of Intelligent Environment to meet Ubicomp Infrastructure needs</td>
<td>Development of an Intelligent Environment Architecture that provides adequate security and privacy to its users. Use of Design Science</td>
</tr>
</tbody>
</table>
Figure 6 demonstrates the relationship between the seven different research activities. The first two research activities are designed to improve our understanding of privacy and security within intelligent environments. Results from these activities are combined with results from the dissertation’s literature review and are used to develop an initial intelligent environment architecture (research activity three). This initial architecture formed a first cut of the required infrastructure, and was used to evaluate user interaction with the environment in research activity four.

The feedback from the design and evaluation of the initial architecture led to the creation of the requirements for a ubiquitous computing infrastructure to support safe user interactions between multiple intelligent environments. These requirements were used to develop the first cut of the final SPACE Architecture (in activity six). The evaluation of the SPACE architecture was used to revise the infrastructure’s requirements (activity five) which in turn was used to improve the SPACE architecture creating an iterative development cycle. These research activities are discussed in more detail below.

### 3.6.1 User Perceptions of Information Sharing

The information shared within an intelligent environment has a huge impact on a user’s privacy. The dissertation seeks to investigate the influences on users’ privacy, and what causes users to share more information within an intelligent environment. This user survey examines the effects of location, trust, reputation and prior contact in the sharing of information and its impact on users’ privacy. From these results we can infer the influence of these factors upon interacting with an intelligent environment, and we can begin to build up our architecture’s design to improve users’ control over their information and improve users’ privacy. This study will then be extended by examining how users interact with their mobile phones, particularly focusing
on their privacy and privacy risk mitigation behaviour. This research activity is described in section 4.2. This research activity received Griffith University Ethics approval (GU Ref: CIT/03/03/HREC).

**Goal:** The goal of this activity is the examination of influences on user privacy within ubiquitous computing environments and of the perceptions of users towards the exchange of information between the user and a wide range of third parties.

**Description of Research Activities:** This research will involve the use of a questionnaire to examine user privacy opinions on mobile communications and information sharing within intelligent environments. The questionnaire will be distributed to a large number of users who have familiarity with mobile phones and PDAs (to ensure adequate understanding of the environments and technical privacy concerns). Therefore this research activity will target early adopters of mobile phones and users within the IT industry.

**Expected Outcomes:** The expected outcomes of this research activity are a better understanding of how users perceive threats to their privacy and how information sharing within intelligent environments can be better designed and supported. This may include a list of the negative or positive influences on a user’s desire for sharing information, and an idea of what structures might be required to provide users with appropriate feedback on information exchanges within these environments. This should further frame the boundary justifications for the dissertation and identify what should be part of this study.

**Research Questions:** This research activity addresses the following research sub-questions:
- How do intelligent environments impact on a user’s privacy?
- How do users interact within an intelligent environment?

3.6.2 Personalisation in Intelligent Environments

The value of intelligent environments lies in their ability to provide users with context-aware services and new community interaction possibilities via ubiquitous computing technologies or environments. Results from previous research activities and existing intelligent environment developments suggest that users interacting with intelligent environments may need to personalise their interactions to filter out unwanted services or to manage the exchange of their identity within an environment. This research activity (described in section 4.2) seeks to understand how personalisation should occur in intelligent environments whilst providing the users with the maximum possible privacy protection.

**Goal:** The goal of this activity is to develop how personalisation and identity management can occur within intelligent environments without impacting user privacy.

**Description of Research Activities:** This research activity involves the development of an intelligent environment architecture that provides users with a method of personalising services and interactions without impacting on their privacy. This involves the development of a usage scenario considering...
what information is required by the intelligent environment and how this information is sensed or obtained from the user. This architecture will then be evaluated to determine where privacy problems occur, and these results will feed into subsequent intelligent environment designs.

**Expected Outcomes:** The results expected from this research activity include: a usage scenario to improve the dissertation’s understanding of what information exchanges are required within an intelligent environment; an architecture that describes the relationship between users and the environment; and an evaluation of the designed architecture and any potential privacy pitfalls.

**Research Questions:** This research activity addresses the following research sub-questions:

- How do intelligent environments impact on a user’s privacy?
- What type of security design is required to ensure the integrity of user data?
- How do users interact within an intelligent environment?
- What type of design is required to allow users seamless interaction between multiple intelligent environments?

### 3.6.3 Initial Intelligent Environment Architecture Development

This research activity develops an initial intelligent environment architecture based upon design suggestions from background literature (shown in chapter two) and from the results of the previous research activities (described in sections 4.2 and 4.3). This architecture defines a private and secure method of users interacting with a single intelligent environment, and will be evaluated (see section 3.6.4) and improved upon in further research (see sections 3.6.5 and 3.6.6). This research activity is described in section 4.4. This research activity received Griffith University Ethics approval (GU Ref: CIT/03/04/HREC).

**Goal:** The goal of this activity is the development of a privacy and security aware intelligent environment architecture based upon existing research literature and earlier research activities.

**Description of Research Activities:** This research activity will develop an intelligent environment architecture that protects user privacy whilst still allowing them access to an intelligent environment’s services. Development of this architecture is based upon existing intelligent environment architectures, privacy design guidelines and information security requirements developed from existing research literature (described in chapter two).

**Expected Outcomes:** The expected outcome of this research activity is a privacy and security aware intelligent environment architecture. The developed architecture in this activity will focus on information control and exchanges, but will not define the technical details of the information exchanges, nor will it technically implement the architecture beyond that required for an initial user evaluation. This architecture will be further developed and extended in further research activities.
Research Questions: This research activity addresses the following research sub-questions:

- How do intelligent environments impact on a user’s privacy?
- What type of security design is required to ensure the integrity of user data?
- How do users interact within an intelligent environment?
- What type of design is required to allow users seamless interaction between multiple intelligent environments?

3.6.4 User Evaluation of Initial Intelligent Environment

This research will investigate user interaction within the developed intelligent environment (refer to section 3.6.3) using a mixture of laboratory and field experiments. This will allow the study of user interaction within an intelligent environment and an evaluation of theories on privacy and security within intelligent environments developed throughout the dissertation. This will be an iterative process that will seek to build upon and test the existing intelligent environment until an effective design is identified. This activity is described in section 4.5.

Goal: The goal of this activity is to evaluate theories on privacy and security by examining how users interact with intelligent environments. Specifically this research project hopes to evaluate the privacy and security aware architecture developed in the previous research activity.

Description of Research Activities: This research will involve the interaction of users with an intelligent environment, an evaluation of how users interact with their personal information and how they perceive their information security. Research activities will include observation of users interacting with the environment, investigation of users’ opinions using interviews and questionnaires, and the modelling of information flow to ensure privacy and security requirements are maintained.

Expected Outcomes: The results from this research activity should evaluate the initial intelligent environment architecture, and provide an evaluation of the developed privacy and security aware intelligent environment architecture. This will then be used as the basis for evaluating the requirements for a global ubiquitous computing infrastructure and the dissertation’s final intelligent environment architecture.

Research Questions: The following research sub-questions are considered in this user evaluation:

- How do intelligent environments impact on a user’s privacy?
- What type of security design is required to ensure the integrity of user data?
- How do users interact within an intelligent environment?
- What type of design is required to allow users seamless interaction between multiple intelligent environments?
3.6.5 Development of Ubicomp Infrastructure Requirements

Intelligent environments use ubiquitous computing technologies to provide pervasive computing services to users within a given environment. Understanding how users will interact with the services is essential in allowing the proper framing of the boundaries of this research, as required by the critical heurists research method described in section 3.5.2. The integration of intelligent environments into our everyday lives will be considered from a global level, examining both the roles of ubiquitous computing technologies in our environments and how users exchange information and utilise services.

This research activity considers the requirements of a global ubiquitous computing infrastructure and develops design suggestions for an intelligent environment architecture that could fulfil this role. This research examines the interactions users have with services, the management of a user’s identity within these environments and how information should be exchanged within the greater framework of the ubicomp infrastructure. The design suggestions developed in this research activity will inform on the final architecture design described in the next activity, and are presented in chapter five.

**Goal:** The goal of this activity is the development of design guidelines for an intelligent environment architecture that could form the basis for a ubiquitous computing infrastructure that covers most of our everyday environments.

**Description of Research Activities:** This research activity involves the development of more detailed usage scenarios for the interaction with intelligent environments across the user’s everyday life. This includes the defining of the identity management and service personalisation requirements for users interacting with these environments, with particular attention to user privacy and information security, and the consideration of the potential benefits these environments can provide to the served community.

**Expected Outcomes:** This research activity will develop the requirements for a ubiquitous computing infrastructure that promotes private and secure user interaction with multiple intelligent environments. This infrastructure should be useful in defining how users interact with the environment and should provide guidance for the dissertation’s boundary and requirements for the final intelligent environment architecture.

**Research Question:** The following research sub-question is examined addressed by this activity:

- What type of design is required to allow users seamless interaction between multiple intelligent environments?

3.6.6 Development of Final Intelligent Environment Architecture

This research activity will develop the intelligent environment architecture designed to ensure user privacy and information security whilst interacting with ubiquitous computing environments. This architecture will include a technical description of the architecture, utilised security protocols, descriptions of information exchanges and the definition of all the entities required for widespread implementation. This architecture improves on the
initial architecture’s design (section 3.6.3), and integrates the design recommendations for the ubiquitous computing infrastructure (section 3.6.5).

**Goal:** The goal of this activity is the development of a private and secure intelligent environment architecture that allows users to interact securely and privately with any intelligent environment. This architecture forms the basis for a ubiquitous computing infrastructure that could cover all of the environments with which users would interact in their daily activities.

**Description of Research Activities:** This activity involves the technical development of the intelligent environment architecture from the initial architecture and design goals for the ubiquitous computing infrastructure. Included in this architecture are the used communication protocols, interaction methods, standard data-flows, identity management entities and system modules.

**Expected Outcomes:** Outcomes expected from this research include: an intelligent environment architecture; a specification for the flow and exchange of information within the architecture; and a description of how the intelligent environment architecture would be used to form a pervasive ubiquitous computing infrastructure to bring services to all areas of a user’s everyday life.

**Research Questions:** The research sub-questions addressed by this development include:
- How do intelligent environments impact on a user’s privacy?
- What type of security design is required to ensure the integrity of user data?
- How do users interact within an intelligent environment?
- What type of design is required to allow users seamless interaction between multiple intelligent environments?

**3.6.7 Evaluation of Final Intelligent Environment Architecture**

This final research activity is a user study investigating the developed intelligent environment architecture (section 3.6.6), again utilising a mixture of laboratory and field experiments. This research will allow the evaluation of the service interaction methods, identity management and security used within the architecture. The architecture will also be investigated during this time for technical security or privacy soundness. This activity is described in section 6.3.3. This research activity received Griffith University Ethics approval (GU Ref: ICT/06/06/HREC).

**Goal:** The goal of this activity is to provide meaningful feedback on the success of the intelligent environment architecture in providing private and secure interactions with an environment and its services.

**Description of Research Activities:** This activity will provide user evaluation of the interaction methods and services of the developed intelligent environment. This will be accomplished by providing users with access to intelligent environments covering familiar physical environments. These intelligent environments will provide services to the user, and they will be asked to evaluate the interaction methods, control of identity information and
types of services offered to allow a determination on the usefulness of the intelligent environment in the current environment.

**Expected Outcomes:** The results of this research activity will provide feedback on the service interaction methods and identity management used in the intelligent environment architecture. This feedback will further inform on the architecture’s design, and allow an evaluation of the success of architecture in forming the desired ubiquitous computing infrastructure.

**Research Questions:** This research activity addresses the following research sub-questions:
- How do intelligent environments impact on a user’s privacy?
- What type of security design is required to ensure the integrity of user data?
- How do users interact within an intelligent environment?
- What type of design is required to allow users seamless interaction between multiple intelligent environments?

### 3.7 Fit of Research Method

This research attempts the difficult problem of designing a communication and interaction environment in an undefined, rapidly changing social context. The research problem calls for an understanding of not only the user’s and system’s privacy goals, but also of the user’s interaction requirements and required pervasive computing services. The use of Activity Theory allows the research to focus on the desired tasks of users interacting with the intelligent environments. Critical Heuristics extends this analysis to consider how the goal of multiple intelligent environments impact on the general architecture. Field experiments and user surveys support the investigation into users’ preferences and interaction requirements, and allow intelligent environments to be experienced within the user’s natural environment.

The use of these research methods allows us to develop a detailed understanding of the user’s requirements for interacting with intelligent environments. Chapter five will describe the generic requirements for user interaction and build on existing intelligent environment research to develop design conclusions that will be useful for future development of intelligent environments. These results will feed into the iterative technical design, described in chapter six, which is further evaluated with an additional Field Study.

The intelligent environment architecture will be constructed using the Design Science guidelines. This methodology is particularly effective in examining the messy or ‘wicked’ problems that characterise unbounded social interaction systems like our intelligent environments. A danger of design science is the potential to over-emphasise the technical design of the system, whilst failing to adequately ground the system in its contextual environment. This can produce technically proficient systems that are useless in their operating context. The use of activity theory and the evaluation of our design using field experiments reduce these risks, and provide a better overall grounding of the requirements of an intelligent environment in our social environments.
Chapter Three: Methodological Approach

This research will develop an intelligent environment architecture based upon users’ perceived interaction needs and the need for user privacy and security. But the social nature of these systems, and the fact that they are designed to be integrated into users’ everyday lives, make them difficult to study. Users must have private and secure access to the environment’s services before they will be able to determine the value of these systems. Furthermore it is likely that their most useful applications have not yet been imagined.

Proper investigation of the benefits and social interaction requirements of intelligent environments would require usable systems that provide useful services in place within users’ everyday environments. This would help overcome the barriers of use of intelligent environments (see section 2.4) and allow the observation of users in their natural environment, interacting with the system as part of their daily lives. The dissertation does however provide this initial (private and secure) intelligent environment which could be used in this investigation.

3.8 Summary and Conclusions

This research has adopted the critical research paradigm in order to ensure the consistent analysis of this research’s findings. (The research assumptions that flow from this research paradigm reflect the Interpretivistic nature of the research problem). The related ontological assumptions acknowledge the subjectivity of the selected paradigm and state that the subjects of this research are voluntaristic. The epistemological assumptions for this research are anti-positivism, which suggests the research problem can only be understood through the point of view of the users within the environment. That is, the privacy (and to a lesser extent the security) provided by an intelligent environment architecture is subjective and cannot be evaluated technically. This is reflected in the use of user surveys and field experiments to investigate users interacting with these environments.

The methodological assumptions describe a constructive, nomothetic research task that requires the iterative development of an intelligent environment architecture based upon users’ initial perceptions and their reactions to developed environments. To achieve this we adopt Activity Theory and Design Science methods, informed on by the previously mentioned user surveys and field experiments. Each of these methods is expanded in the Research Design section, which describes the research activities involved in this thesis. The next chapter will describe existing research in intelligent environments, privacy, security and interacting with digital environments.
Chapter Four: Preliminary Investigations into Privacy in Intelligent Environments

4.1 Introduction

This chapter attempts to further develop our view of intelligent environments and their integration into our everyday worlds. It describes the research activities carried out examining intelligent environment design and user perceptions of information sharing and privacy within ubiquitous computing environments. This work builds on known problems with existing intelligent environment architectures, and allows us to develop an architecture that allows users’ private and secure interactions with an intelligent environment.

The initial intelligent environment architecture, described in section 4.4, is an initial prototype that is used to evaluate the environment’s technical and user interaction requirements. The user evaluation of this initial architecture is described in section 4.5. This architecture will subsequently be evaluated (in chapter five) and developed (in chapter six) with respect to the interaction requirements of users within a ubiquitous computing infrastructure. The relationship between these research activities is described in Figure 6 (refer to 3.6).

4.2 User Perceptions of Information Sharing

A user study was conducted to evaluate users’ perceptions of information sharing within an intelligent environment. The information shared within an intelligent environment has a huge impact on users’ privacy. This user study investigates what prompts users to share more information, and what specifically impacts users’ privacy. The study examines the effects of location, trust, reputation and prior contact in the sharing of information and its impact on users’ privacy. The results can be used to infer the influence of these factors upon users interacting with an intelligent environment.

These results allow future user studies to be adapted to explore the findings further and to validate them in another setting, improving their generalisability. These results are ultimately incorporated into the dissertation’s architecture to improve users’ control over their information and subsequently improve users’ privacy. This study's breadth also allows the investigation of impacts upon a user within an intelligent environment. This allows further consideration to the correct conceptual boundary (see section 3.5.2.1) of the dissertation's research questions (and helps to identify the required infrastructure that is defined in chapter five).

4.2.1 User Study Description

Questionnaires were distributed among Australian university students participating in information technology courses (in first and second year) and throughout the ICT faculty. This user group was targeted due to their...
accessibility, the likelihood of these participants having experience using mobile phones and understanding the underlying technologies described in the survey, and because this group was expected to be early adopters of interactions with ubiquitous computing environments. The questionnaire was returned by 119 participants, aged between 17 and 40 and predominantly men in their twenties. The user group showed interest in the project, and the return rate for the questionnaire was approximately 80%. No compensation was offered for this study.

The multiple-choice based questionnaire was designed to measure users’ privacy opinions on mobile communications and information sharing within intelligent environments. One hundred and fifteen of the participants (or 97%) reported owning a mobile phone, while no one reported sharing their phone with another person. This result is likely to be dependent upon the prevailing culture and socio-economic level of the respondents. Further information on this study can be found in (Chatfield & Häkkilä, 2004).

Further evaluations were conducted investigating users’ perceptions of privacy whilst using mobile phones. Ten user interviews were conducted, including the original survey questions and more focused questions investigating the subtler privacy concerns of users while using text messages. As we focused on users’ privacy perceptions of SMS communication, the criterion for selected participants was that they were active SMS users. The five Australian and five Finnish participants were not offered any financial compensation for taking part in the experiment. Further information on this study can be found in (Häkkilä & Chatfield, 2005).

This study explores Mobile Phones usage along with information sharing within intelligent environment. While this could be said to prejudice some of the results, this dissertation argues for the use of the mobile phone in interaction with intelligent environments due to their pervasiveness and user familiarity. Intelligent environments will become logical extensions of the smart phone interactions that occur today, and therefore users attitudes to user privacy and encryption on short message exchange services is very relevant for this dissertation.

### 4.2.2 User Study Results

Participants were first questioned on sharing personal information with a service provider. Table 10 describes characteristics that would make the users more comfortable with sharing their information. Approximately half of all respondents selected a preference for clearer feedback describing what the information will be used for, and who will have access to it. Table 11 describes the influences identified by the users as affecting what information they would be willing to share. The relatively low level of influence seen in these results, i.e. no strategy was supported by more than 33% of respondents, suggests users are generally unwilling to share personal information with an intelligent environment. As participants were advised to select all the options that applied for each question, the sum of the results exceeds 100%.
Would you feel more comfortable disclosing information if you could clearly see:

| What the information will be used for | 52% |
| Who will have access to the information | 47% |
| All information you provided was recorded anonymously | 29% |
| Where the information was being stored | 26% |
| How information is being gathered | 23% |
| How long the information will be stored before being erased | 21% |
| None | 13% |

Table 10: Influences on Participants Sharing Personal Information

When would you be more likely to share information with a service provider?

| Could request your information be deleted | 33% |
| The service provider had a good reputation globally | 32% |
| All information you provided was recorded anonymously | 29% |
| The service provider has a clear, easily accessible privacy policy | 25% |
| If you considered the service rendered to be especially valuable | 19% |
| None of the answers | 19% |
| The service provider was recommended to you by your friends | 8% |

Table 11: Information Sharing Likelihood For Different Influence Factors

The questionnaire next inquired about users’ desire to control the information shared with their environment or an external person. The question described a scenario where information could be automatically shared between the user’s phone and the environment, a case common in intelligent environment and ubiquitous computing research:

Each time someone wants to access your information, they have to send an information-sharing request to the database. Each request is considered separately in order to decide if the information request is answered or not. Would you prefer requests for information to be handled by:

a. Default settings on your mobile phone

b. Individually approving each exchange

c. Combination of the two

Only 17% of the participants chose to automate the information exchange with the environment. 38% indicated they wanted complete control, while 45% selected a combination of the two. These results mirror the later findings of Iachello et al. (2005) in their investigation of information sharing using a peer-to-peer, mobile, location-enhanced messaging service. The authors found that automatic system messaging between participants wasn’t required.
or desired. These findings suggest automatic information sharing should be minimised or eliminated within ubiquitous computing environments.

The final question of the survey was an exploratory research question seeking to identify with whom users would be most likely to share information, and under what circumstances. The goal of this question was to contribute to the direction of future research on user information sharing preferences and automated information sharing systems. The information that was available to share was as follows: *Name, Alias, Contact Details, Primary and Secondary Email Addresses, Interests, the user’s Approximate and Actual Location and their Current Activity*. Users were asked to highlight which information they would share with different types of people they had met, service providers that might be within the environment and with other organisations the user might know.

Since it was an exploratory question, the authors sought to identify which of the different user types caused the subjects to share more information. To determine this, each selection was considered separately in relation to the subject’s responses to other user types, as people clearly had individual strategies for information sharing. For example, we expected that within close social groups, users would share all their information with their family and almost everything with all the other groups, whereas other participants would share only their name with everyone else. Thus, we chose to determine the relative change in information shared to determine which groups were identified the most.

Four user categories were used as positive reference values: *family members, friends, associates and employers*. A *stranger that provides you with no personal information* was used as a negative reference. The aim was to indicate which of the other user groups could be used to influence personal information sharing systems and how these groups behaved in comparison to the reference groups. The question therefore sought to identify which of the categories influenced the participants the most. A category was considered to have influenced the user if they indicated they would share more information with them than with a stranger that shared no personal information. More information was considered in this case to be another piece of primary information (*Name, Contact Details, Primary Email or Actual Location*), or two pieces of secondary information (*Alias, Secondary Email, Interests, Approximate Location or Current Activity*).

Of the 119 participants, 22 left the question blank, indicating they would either share no information with the environment, or that they did not wish to answer the question. The results described in Table 12 represent the remaining 97 participants. These results show users are much more likely to share information if a prior relationship (either business or social) exists between the user and the third party. There is also interest in the reputation of the third party, which highlights the need for reputation systems to augment the trust relationship normally developed through repeated interactions.
Chapter Four: Preliminary Investigations into Privacy in Intelligent Environments

<table>
<thead>
<tr>
<th>User Types</th>
<th>n = 97</th>
</tr>
</thead>
<tbody>
<tr>
<td>Someone you met previously at a social function/party</td>
<td>59%</td>
</tr>
<tr>
<td>Someone you met previously at a business function</td>
<td>57%</td>
</tr>
<tr>
<td>Services you have subscribed to (e.g. Auto Club, Directions providers, etc.)</td>
<td>57%</td>
</tr>
<tr>
<td>Stranger who is a friend of a good friend</td>
<td>40%</td>
</tr>
<tr>
<td>A stranger, or organisation, with a good reputation (e.g. Red Cross, Amnesty)</td>
<td>40%</td>
</tr>
<tr>
<td>Stranger that provides you with most/all of their information</td>
<td>31%</td>
</tr>
<tr>
<td>Stranger that is nearby (e.g. in the same room)</td>
<td>29%</td>
</tr>
<tr>
<td>Nearby Information Providers (e.g. Information Booths, Advertisers)</td>
<td>24%</td>
</tr>
</tbody>
</table>

**Table 12: Different User Types and Results for Information Sharing**

Further investigation of mobile devices considered how private respondents considered their mobile phone to be, and sought to understand the effects of the perception on users’ interactions with their phone. 82.3% indicated that they considered a mobile phone to be a private device (23.5% indicated ‘Very Private’, and 58.8% responded ‘Somewhat Private’). 14.3% did not consider a mobile phone to be a private device. Three survey responses were left blank.

The interview results tell a similar story, with users equating their mobile device as private as a personal letter or their wallet. User comments from the interviews gave strong indications on widely accepted norms of treating other people’s phones as their intimate gadgets:

‘The thing is that nowadays nobody likes to give their phone into someone else’s hands. Text messages, phone calls, photos, emails, all your life is there.’ (Interview Subject #10)

This identification of their mobile phone as a private device was especially highlighted when we investigated whether users would allow others to answer their phone (either phone calls or text messages). The results, in both the questionnaire and in the user interviews, overwhelmingly indicated that this was not an acceptable practice. The study identified that text messages were much more private than phone calls, as the subjects were twice as reluctant to allow others to answer their text messages (60.5%), compared with normal phone calls (30.0%). Five participants compared text messages to letters, and noted the ‘privacy of correspondence’ related to letters was also valid for text messages:

‘There cannot be such a situation [that someone reads your message before you]. If someone opens your message, he or she must be extremely interested in your doings and does it on purpose. It is a violation of privacy; it’s like if you opened someone else’s letter.’ (Interview Subject #7)

Further investigation of this during the interviews revealed that we as a society have developed a number of social etiquette rules to mitigate risks to
our privacy. Users describe the privacy expectations that they have while using text messages that are shared amongst their social group. Other participants described strategies that they used to ensure their privacy through the text used in the message, such as using colloquialisms, code words and even another language, or by deleting messages as soon as they are received to safeguard the senders’ privacy. However, seven participants reported that they did not use any strategies to improve privacy, but instead relied on the recipient, whom they trusted, to understand the privacy level of the message. Five participants responded that they were really not interested in privacy adding features or security, as their practices already employed the assumption that the messages were private, and saw that the general SMS culture respected this rule.

Finally, the interviewees were asked two questions exploring ideas for improving text message privacy. The first asked whether they thought it would be useful to be able to send additional privacy information with the message. The example given was an icon next to the message in their message inbox that indicated how private the message was. Three participants responded that they saw it as useful, whereas the remaining did not see it being necessary, as the phone was already understood to be a personal device.

The second question asked if the use of encryption to secure a text message would be useful. The responses to this question were mixed. Four users, all of whom were from Australia, agreed that this would be a valuable service. None of the Finnish participants were interested in encryption of their messages. One user did comment that they saw value in authentication of the correct receiver, for instance with PIN code, fingerprint sensor or using voice authentication. The five participants doubting the usefulness of message encryption commented that it would not improve the current practice – that is, it was up to the receiver to ensure that the message remained private as they could still show it to a third party.

The view, then, was that encryption would not change participants’ behaviour with SMS messaging, as existing social practices were sufficient to ensure user privacy. In addition, three participants expressed concern over additional input methods: they would not like to have additional steps or extra dials when they wanted to send or read a message. Three other participants commented that, if encryption were possible, it might change the use of text messages in some circumstances, e.g. for confidential business purposes, but it would not change their own practices. An Australian participant rejecting the encryption idea cited that he/she was suspicious of new features that could add an extra expense to the service. Instead of encrypting messages, one participant suggested requiring authentication from the correct receiver before opening the message, for instance with PIN code, fingerprint sensor or voice authentication. Another suggestion called for the automatic deletion of messages to be supported, allowing users to set how long the recipient had to read the message before it was deleted, e.g. read once, delete after two days etc.
4.2.3 Discussion and Design Conclusions

This user study examined likely early adopters of ubiquitous computing technologies (a mostly young, technology-focused audience) who are representative of the users who will eventually use intelligent environments (given that intelligent environments are unlikely to appear in the near future). This representation is consistent with the expectation that our sample for the field study will not provide a representative population distribution (Cunningham, 1997; McMurray, Pace & Scott, 2004). Whilst it is not feasible to develop a field study that is representative of the entire population, the results were validated through the examination of existing literature, by conducting further user studies in similar environments and by examining the collected data for contradictory results. This validation identified no contradictory results from literature or the dissertation's other user studies (see sections 4.3, 4.5 and 6.4.2). Further research that could validate these results is described (as an extension to the dissertation) in section 8.3.3.

The results of the ten user interviews are consistent with the user questionnaires in terms of phone ownership and perceptions of user privacy. The interviews therefore provide some insight into the reasons for the survey answers, and the additional commentary from users provided valuable insights into how users perceived their mobile device, and how they were likely to want to relate to this device in ubiquitous computing environments.

The high percentage of users (83%) wanting control over the exchange of their information could indicate a level of distrust with automating the exchange of sensitive information. With intelligent and context-aware systems, the potentially uncontrolled transmission of the user’s data to the system infrastructure has already given rise to concerns (Barkhuus & Dey, 2003). Users want to stay in control over the information they share, and are concerned about their privacy and the exchange of personal information.

Ubiquitous computing environments must provide clear feedback on how, why and with whom their information is being shared. Users want to know where the information is being stored, how it was gathered and how it will be maintained. They also want access to the intelligent environment’s privacy policy to help them assess the risk versus reward of accessing an intelligent environment’s services. But most of all users want control over their interaction with the environment and want to be allowed anonymous interactions with the environment.

This study also found that an existing relationship between the users of an intelligent environment is the biggest influence on user information sharing. This is true for both individuals (a person the user had met) and organisations (a service which the user had subscribed to). These findings are consistent with Zheng et al.’s (2002) research suggesting initial contact between users at social activities can jump-start trust relationships. These results suggest that a user model should identify whether a prior relationship exists before any information exchange.

The importance of the prior relationship is seen also from the results concerning organisations, as users were more willing to share information
with the services they had subscribed to than, for example, services nearby. This suggests that reputation is also important when no prior relationship exists. This supports Goecks and Mynatt’s (2002) findings that trust and reputation systems could prove valuable for allowing users to build trust and make better use of an intelligent environment.

A third party’s willingness to share information, or their organisation’s physical proximity to the user, seems to have very little influence on a user’s desire to provide them with information. This could be perhaps because in this case there is no expectation of a future relationship. An established relationship would suggest that one would exist in the future. While these results are indications of users’ desires in these environments, there is often a disparity between what users claim they desire from a system and their actions whilst using the system. See for example the differences between users’ stated privacy preference versus their actual behaviour in E-Commerce systems (Berendt, Gunther & Spiekermann, 2005).

In order for users to have control over intelligent environment information, there must be recognition of the ownership of information collected within, and generated by an intelligent environment. This research suggests that users would prefer that information be owned by the entity it describes or that provided it. Users should retain ownership of any personal information; interactions with an intelligent environment (e.g. the personalised interactions between a user and an environment’s services) should be owned by both the user and the intelligent environment, and the information generated by the intelligent environment (i.e. usage statistics describing all users that interact with environment) should remain the property of the environment’s owners.

This allows both parties access and control over their information. An example of this in action would be an intelligent environment that would only be allowed access to users’ personal information when the user is interacting with the environment, but would allow access to their service personalisation information at any time. Likewise users could access this personalisation information, and should have access to, and control over, any of their personal information stored within the environment. This control of information is examined in section 5.2.4.

Users’ privacy is guarded by widely accepted, unwritten rules of treating mobile phones and messages as confidential. Text messages in particular are considered very personal, as the lack of any ‘context of privacy’ sent with a message ensures that most users treat all messages as private. These strong social norms indicate that text messaging is not comparable with any other electronic communication medium, e.g. emails (which are commonly forwarded without the sender’s permission), but are more comparable with traditional letters. The interviews demonstrated some support for the use of encryption or for additional privacy information to be sent as part of a text message. However these tools were rejected by many participants in favour of the social norms that currently preserve user privacy.

Findings from the user interviews and survey questions suggest that privacy of users’ information stored on a mobile device is protected by the social
norms and rules that govern their use. So while this research supports the use of encryption and other security techniques for interactions between users and an intelligent environment, users should only use additional security measures on their mobile device if they feel that it is insecure. This suggests that the securing of a personal mobile device is not a design priority, given the social rules that govern their use. The dissertation should instead focus on securing the exchange of information within an environment, and the security and privacy structures required to allow interaction and use of ubiquitous computing services without eroding users’ privacy.

4.3 Personalisation in Intelligent Environments

Personalisation occurs when a user accesses the services provided by an intelligent environment. The personalisation allows the limiting or highlighting of the services presented to the user by the environment, based upon the users’ stated preferences or in response to the users’ previous behaviour. Personalisation allows us to overcome the ‘invisibility problem’ (see section 2.3.5), or to limit the users’ access to information that is relevant to them. But the personalisation of an intelligent environment’s services requires access to these personal profiles or interaction histories, and this collection of information can cause users significant privacy problems. This section explores these issues and makes design recommendations for personalisation in intelligent environments.

4.3.1 Intelligent Environment Usage Scenario

A scenario was developed to better explain how a user would interact with an intelligent environment. This allowed workshop participants to discuss the privacy aspects of interacting with an environment from a common understanding of the environment’s purpose and user’s motivations for service usage. The scenario was particularly useful for examining the flow of information between the user and the environment, and was subsequently extended to describe other aspects of the intelligent environment architecture (as seen in sections 4.4 and 5.2.1.4). The impact of the workshop discussions on our personalisation design is described in the next section.

Consider the example of Belinda, a young IT professional, who works near a large shopping mall. Both the mall and her office have intelligent environments that can provide information to her mobile device. Each environment contains pervasive computing devices that detect users within the environment, and seeks to provide them with relevant information based upon who the user is and what their interests are. In the case of the shopping mall, directions to particular merchants can be provided, as well as a list of sales that might interest the user. The more private intelligent environments in Belinda’s office can provide limited directions and can be used by employees to locate their colleagues.

In each situation Belinda may want to vary the way she interacts with the environment. In the shopping mall she may have different interaction goals, e.g. shopping or using nearby public transport. For each of these goals she could use a different persona containing her preferences for shoes or...
transport routes, and these personae will likely have no identifying information. At work Belinda is likely to need multiple personae to reflect the different roles she adopts in the workplace (e.g. substantive position, acting up, fire warden, selection committee member, or person responsible for a particular visitor), and will surely identify her to the environment. The following section describes an architecture that could be used to manage these interactions in a private and secure manner.

### 4.3.2 User Interactions with the Intelligent Environment

Intelligent environments provide personalised services to their users by gathering data on the current state of the environment. This information is used to build a World Model of the current context of the environment, which in turn is used to personalise the interaction that a user has with the environment. Figure 7 describes a generic intelligent environment architecture that demonstrates the flows of information within the environment. This architecture is based upon the Merino intelligent environment architecture (section 2.3.2.1) and has attributes in common with most intelligent environments that use a mobile device for service interaction.

**Figure 7: Secure Intelligent Environment Architecture**

The intelligent environment architecture is comprised of two sections: the Intelligent Environment, and the users’ system. The World Model contains logs of all sensor activity and a representation of the current context of the environment, e.g. the office intelligent environment would know the current location of each employee. The Access Control Manager is used to manage
the distribution of information to the users, including the personalisation of the interface sent to the user’s device for both user and service interaction.

The User System includes the user’s handheld device, Identity Manager and Personal System. The user’s device holds their viewing preferences and provides access to their personal system. Personalisation could potentially occur on either the user’s device, by loading the interface from the access control manager and personalising it using the user’s preferences, or on the access control manager, by loading the user’s preferences from their device. An example of this interface is the MyPlace Visualisation Interface, described in section 2.3.2.5.

The Identity Manager allows the user to store different personal identities with which to interact with the environment. This is stored on the user’s device to limit the systems access to user information, and to allow the user to interact with an intelligent environment without requiring the user to first set up an identity account. The User’s Personal System provides personal information to the environment and other users in accordance with the user’s privacy preferences. These elements could logically be stored on the user’s handheld device, or maintained in a third location that is contactable by both the user’s handheld device and the intelligent environment.

This design provides a method of personalising the user’s interactions with the intelligent environment, but it also raises security and privacy questions surrounding the control of information and the personalisation process. A common problem within systems that track their users is the ability to search for a user’s activities over time. This occurs when a unique identifier can be linked to a particular user and when sensor logs are made available to a tracking system. To prevent this problem from occurring, users need to use temporary IDs to protect their privacy. A temporary ID is assigned to a user when they first connect to the intelligent environment, and that ID is only valid until they leave the environment.

In our example, the first interaction that Belinda has with either intelligent environment is when her mobile device is discovered by one (or more) of the many sensors. Her MAC address would be logged as a global, unique ID for her device and forwarded to the intelligent environment’s World Model. This MAC address is then exchanged by the User Identity Manager for a temporary user ID, and that user ID links all interaction with the ID (information requests etc.) to the user’s device through the linked MAC address. This means that, even if a previous temporary ID for a person was known, there could be no historical location tracking, as the link between the user’s MAC address and the temporary user ID is not stored or made publicly available. However this method relies on the network being trustworthy in its use of the user’s MAC address, something that cannot be guaranteed.

The Access Control Manager is responsible for controlling access to both the environment’s users and services. Information is distributed based upon the identity of the users interacting with the system. To do this the Access Control Manager would request identity information from the user. This request would be evaluated by the user’s personal system and return information ranging
from no information to verifiable ID. The intelligent environment would then provide a subset of the intelligent environment’s worldview based upon what the user is allowed to access.

But this initial view of access control in intelligent environments makes many assumptions. It assumes that the user would want to use the same identity not only with multiple services, but also with other users. Conditional identity management delivery, including the decision of the user as to whether to provide any identity information, was identified as essential by the initial user study (in section 4.2). Similarly, this access control method also assumes that users will always want to interact with both users and services. Future designs should separate these functions allowing separate (and when required, anonymous) interaction.

The provision of identity information to the environment is used to personalise the information returned during service interaction. To reduce the information stream sent to the user’s device, preferences and selected personal information (i.e. the user’s ‘identity’) forwarded to the environment would be used by the Access Manager to eliminate aspects of the returned interface. For example, if Belinda was shopping for music or computers, her device could relay these preferences to the shopping mall’s Access Control Manager and it would only present sales information on these topics. This allows the user to remain in control of their information and only share what is required for a particular service or personalisation. In this intelligent environment model, some of this identity information would be provided to other users in the environment, allowing them to interact with the user.

This personalisation method will, however, cause problems with user privacy. Services may require more personal information than the user would want to share with other users. It also implies that users should automatically have their identity information shared with other users, something rejected by the initial user study (in section 4.2). Finally it requires the user to give up personal information in order to improve service delivery, when privacy design strategies clearly call for the reduction (or elimination) of information flows from the user where possible. This intelligent environment architecture must be improved to allow the user to act anonymously unless there are clear benefits for not doing so.

4.3.3 Discussion and Design Conclusions

The evaluation carried out on the generic intelligent environment architecture described in Figure 7 has led to the many design improvements that will be incorporated in our initial intelligent environment architecture. The most important changes are the ability of users to interact anonymously with the environment, the need to interact with the environment’s users and services separately, and the need for a more effective personalisation system to drop the requirement of the user exchanging identity information with the environment before any interface personalisation can take place.

Providing anonymous interaction with an intelligent environment requires a number of changes to the presented generic architecture. Firstly the design
suggests that upon entering the intelligent environment the user’s mobile
device is detected by the environment. This gives the environment access to
the user’s MAC address, which has the potential to be misused however the
services are designed. And even in the event that all the environment’s
services were trustworthy, and the environment’s developers had put in place
the safeguards mentioned above, users still would not know they could trust
the environment. Ideally this system should be replaced by user-initiated
discovery of intelligent environments. Services and user interaction spaces of
intelligent environments should be discovered separately.

This change would allow users to be more selective of how they represent
themselves to the environment. Instead of users being ‘discovered’ by the
environment, and potentially recognised from previous interactions, they can
choose how and when they want to interact with the environment. Users
could utilise different profiles and interaction histories for interacting with a
particular environment in a particular way. For example, a user might have
one interaction account for interacting with a public service, another holding
their news searching preferences and a final profile for secure interaction with
their employer’s intelligent environment. This identity management would be
especially useful as the numbers of these environments covering the same
area increase. Services may, however, require external evidence of identity,
beyond that provided by the user, and this would need to be through external
independent identity brokers accessible via a common interface (e.g. via the
Internet).

Personalisation of the service interface must not require that users provide
identity information upon connecting to the intelligent environment. By
allowing the environment to collect information on users’ habits, preferences
and previous interactions, users open themselves up to all sorts of privacy
concerns. A more effective method would allow users to control their own
personalisation information by storing their information and personalising the
interface on their own handheld device. This creates different design
problems, such as the additional bandwidth required to download the entire
range of services or interface options before the personalisation is complete
on the local device.

This client-side personalisation is similar to the personalisation utilised by the
BlueStar intelligent environment, described in section 2.3.5. This allows the
users personalised service delivery without requiring them to give up valuable
personal information. This client-side personalisation should be used wherever
possible in intelligent environments, and we should develop other methods of
interacting privately and securely when this method of personalisation is not
available for technical (e.g. bandwidth) or security reasons (e.g. services that
require identity authentication).

### 4.4 Initial Intelligent Environment Architecture

This section describes an interaction framework for users within an intelligent
environment, and between users and the environment’s services. This
extends the architecture presented in the previous section, and considers
what interaction both the users and intelligent environment need to have with
external entities to allow secure and private interactivity. This architecture is an initial prototype that is subsequently improved in later chapters (refer to Figure 6). It was developed by the dissertation author and was originally published in (Chatfield & Hexel, 2004).

4.4.1 Privacy-Aware Intelligent Environment Architecture

This section describes an initial architecture that allows users to have private and secure interactions with an intelligent environment and its services. Initial investigations into the architecture’s design requirements (see section 4.2) highlighted many users’ privacy concerns when sharing information using ubiquitous computing technologies. Areas of particular concern are who will have access to the information and what the information will be used for. An intelligent environment must have a clearly accessible privacy policy, allow users to choose how they interact with the environment and its services (i.e. provide anonymity), and maintain a method of personalising current services and interactions based upon previous experiences. This requires a method of securely using users’ interaction histories and confirming the user’s identity with the environment.

The second investigation (see section 4.3) identified a number of design goals that have been included in this intelligent environment architecture. The first relates to the need for anonymous interaction with the environment and the need to prevent the intelligent environment from collecting any information about the user without their express permission. Similarly, the personalisation of a user’s interaction interface must be possible without requiring a user to give up personal information. This satisfies privacy design strategies calling for a reduced information flow from the user and allows the user to have the same interactions that they would in the real world.

Related to this is the need for the user register and services to be discovered separately and allow the user to use different identities for each. This allows users to share different information with environment users and services, and enables the user to provide different user identities based upon the interaction required in a given situation. This is an important aspect of maintaining users’ privacy when interacting within an intelligent environment.

The privacy-aware intelligent environment architecture (Figure 8) describes an interaction framework for users within an intelligent environment, and between users and the environment’s services. The architecture is based upon existing research in user privacy, calling for user control of their personal information and any information exchanges, identity management, requiring external confirmation of identity separated from the environment, and security. The architecture allows all users to remain anonymous, sharing only the information they choose with the environment and other users. It is assumed that all information passing through the intelligent environment is secure, and no recording of user details is carried out.
This architecture is comprised of two main parts: the user register and service providers that comprise the inner workings of the intelligent environment; and the identity manager and identity broker that manage access to users’ information and personal details. Figure 8 shows the interactions users can have within the environment, either directly with the user register or service provider, or indirectly with another user through their identity manager. The user register and the service provider are separated to prevent information from being reused by another environmental entity without the user’s knowledge or consent.

To guarantee user privacy, an intelligent environment must secure all user information and all references to user identity. To ensure that these references are secured, the intelligent environment temporarily assigns each user in the environment with an alias. This alias can be used to request information about the user from the user’s personal domain through an identity manager. This design allows responses to these queries without the need to contact (and potentially identify) the user’s mobile device. This is useful to reduce the computation burden on the user’s mobile device (and the wireless communication bandwidth), and allows these queries to be performed when the user is out of direct contact with the environment.

A user’s personal domain is a user-controlled server that allows the user to maintain a representation of themselves on the Internet which can respond to queries about the user (e.g. their location, personal details, ability to receive electronic or voice communications etc.). Each user’s personal domain contains (amongst other information) the user’s profiles that are displayed for different types of users. A user modelling tool similar to the Personis user modelling system (Kay, Kummerfeld & Lauder, 2002) could be utilised to provide different audiences with different user profiles. The design of a user’s personal domain is further examined in section 6.2.4.

Users interact with the intelligent environment using some form of unique identifier (e.g. the user’s MAC address). Request for information on another...
user is made through their identity manager (see Figure 8). This request is processed through the intelligent environment, which securely exchanges the user's temporary alias (received from the user making the request) with their unique identifier (to be passed to the identity manager). Users could provide the intelligent environment with a pseudonym if they wanted more identifiability, or could utilise a randomly-generated ID for greater anonymity and protection against tracking or historical searches (as demonstrated in (Gruteser & Grunwald, 2005)).

The identity manager takes the user’s unique identifier and directs the request to the user’s personal domain. This domain will then securely provide a selected profile based upon the user's privacy preferences and the identity of the inquirer. The results of this information request are again passed through the intelligent environment, ensuring that no identifying information (beyond that provided by the user) is available to the inquirer. Trust and reputation could be used to enhance the effectiveness of the user's privacy preferences, allowing less rigid and more user-friendly control and distribution of the user’s personal information.

Upon entering an intelligent environment, details of the available services are broadcast by any available intelligent environments and displayed on the user's mobile device. To take advantage of these services, the users must (either actively, or through the setting of personal preferences) provide a service request, and any required information, to the intelligent environment. If a service requires verifiable information, users can make use of a third party Identity Broker to verify user information in a secure way. An Identity Broker is an accredited third party that maintains an account verifying some or all of the user information (e.g. VeriSign’s Consumer Authentication Service (http://ww.verisign.com/), Liberty Alliance (http://www.projectliberty.org/)).

An identity account enables external systems (e.g. intelligent environments) to confirm necessary details about the user (e.g. name, age, etc.). This system works in much the same way as an electronic ID card issued by a trusted source (e.g. a bank or government department). So whenever a user wants to prove his identity, he simply provides a secure key for the system to query. A user could potentially have multiple relationships with an identity broker, each representing a different persona, or a different subset of their personal information. To further facilitate user privacy, an identity broker should only provide the minimum information necessary to authenticate the request (e.g. confirming that the user is over 18, but not providing their birthday).

For trustworthy information to be stored at the identity broker, a user must first set up an account. Depending on the account type, and the information being verified (e.g. financial payment, proof of legal name, allergies etc.), additional verification of the facts managed by that account may be required. This would be handled through the provision of verifiable data through independent channels such as the inspection of a photo ID, the collection of a digital photo or fingerprint etc. The intelligent environment should not store this verification information, but should instead route it between the
institution that maintains and verifies the account and the requesting systems.

4.4.2 Discussion and Design Conclusions

The initial intelligent environment architecture describes how users interact with environmental services and other users. This architecture uses external entities to provide confirmation of identity and to exchange information between users without exposing unnecessary information to the intelligent environment. Interactions between environments are managed on the user’s mobile device, which can select different interaction profiles for users depending on the environment and the services required. The interaction with an environment’s users or services is managed separately. A review of this architecture does suggest potential improvements and areas where more understanding is required.

This architecture supposes that Internet access will always be available for access to required identity authentication structures. When this is not the case, users may need an alternative method of proving their identity to the environment or its services. Users may also want to utilise pseudonyms that only contain partial personae or a subset of their personal information. For example, a user might want to prove they are a member of a club or organisation but not give their name or address. This ability is attractive because it mimics real-world interactions that allow users access to a service whilst maintaining anonymity. Future iterations of this intelligent environment architecture examine the use of digitally-signed user personae (described in section 2.4.5.1) to provide this functionality.

User interaction within this intelligent environment still requires more investigation. A cursory analysis of user interactions with this initial architecture reveals a problem with users using a persistent identifier when interacting with the environment. These identifiers can be used to connect different interaction sessions and create a detailed profile on the user, something that is not acceptable from a privacy point of view.

This research must consider what happens when users enter an intelligent environment without a mobile device. It also requires a better definition of how two users interact through the intelligent environment. User interaction within an intelligent environment is explored in more depth in section 5.2.4. The impact of information storage (and in particular the securing of user interaction information) on users’ privacy also requires more investigation. This is explored in section 5.2.5.

Intelligent environments are often publicly available and have additional vulnerabilities based upon their use of ubiquitous computing technologies (like being susceptible to physical tampering or hacking). It is therefore important to consider what would happen if each aspect of the environment was compromised by a malicious entity. The User Register and IE Services (described in Figure 8) gather personal information about the users, so a breach in either of these could be a potentially devastating to a user’s privacy. The Service Provider in particular is likely to have information to personalise
service delivery and assertions of identity. To reduce the risk to user’s privacy, an intelligent environment’s services (and the user register) must store information encrypted, and personal information should only be readable when in direct contact with the user. These concepts are investigated in section 5.2.5.1.

Both the Identity Manager and Identity Broker in this architecture are ‘trusted’ third parties that either perform identity authentication or enable the authentication process (in the Identity Manager’s case by routing information requests to the Personal Domain). These entities will be heavily secured, but a breach is still possible. A breach in the Identity Manager would provide information on users of the service and the address of their Personal Domain. The manager’s database may not have user names, and as the identity manager account number used in an environment is always encrypted this breach is unlikely to be too damaging. A breach in an Identity Broker on the other hand could reveal complete information on a user’s identity. Identity Brokers will therefore be selected by users based upon their perceived ability to remain secure. A Personal Domain could equally store complete user information, depending upon what the user uses it for. As the personal domain is user controlled, these risks would be mitigated by the user only placing limited information on the Personal Domain. Users will need to understand the likelihood and risks of these breaches if they are to be able to make these privacy decisions about use and information storage within an intelligent environment. See section 6.2 for more privacy threats discussions. Intelligent environments may be hosted in areas with other similar environments, all with potentially numerous services that must be accessed across the same wireless network. This will require a flexible, scalable infrastructure that can be used by mobile devices with limited wireless bandwidth. The privacy and security of this infrastructure and the storage of users’ information within an intelligent environment are considered in the final architecture’s design. The method by which users identify and interact with intelligent environments is described in section 6.2.2.

This architecture is evaluated by means of a user study (see section 4.5), and this forms the basis of our ubiquitous computing infrastructure discussed in chapter five. Of particular interest are the services that will be offered using ubiquitous computing technologies, the personalisation of users’ interactions with these environments, and the effect of different information sharing on the user’s privacy, information security and identity brokerage. The final architecture is described in chapter six.

### 4.5 User Studies of Initial Architecture

A user study was carried out using the MyPlace Visualisation Interface (MVI) (refer to section 2.3.2.4) to examine the invisibility problem and users’ perceptions of privacy and information sharing within intelligent environments. User privacy within intelligent environments is impacted when users’ information crosses a personal border of privacy (e.g. physical, social or temporal borders) (Langheinrich, 2002). This study examines the effect of information flowing across physical borders, within certain social groups and
outside of temporal borders. The boundary justifications (see section 3.5.2) identified for the dissertation’s research questions are also explored by this user study.

Any environmental impacts on users’ privacy and security perceptions are added to the analysis of the problem domain in chapter five. As part of the boundary justification analysis, this user study examines other known impacts on users within intelligent environments. It therefore considers the influences of trust and reputation (identified as important in a previous user study (section 4.2.2) and by other authors (Goecks & Mynatt, 2002)) and user anonymity on users’ privacy (Langheinrich, 2001).

The results from this user study provided privacy and security design requirements for the management of information and the personalisation of services within an intelligent environment. These results are used to evaluate the initial architecture described in section 4.4 and form the basis for the ubiquitous computing infrastructure described in chapter five. The relationship between this dissertation’s numerous research activities are described in Figure 6. This user study was developed and conducted by the author of the dissertation. It was originally published in the Australasian Computer-Human Interaction (OzCHI) 2005 conference (Chatfield et al., 2005).

4.5.1 User Study Description

A user study (N=17) was conducted to examine users interactions within a simulated intelligent environment covering a university common area using the MVI. The approach adopted had characteristics in common with both a laboratory experiment and a field study. The common area was selected as an area the users would be familiar with. This area could potentially hold services that would be useful to the users (e.g. printing, directions to facilities, etc.). The users were given a brief orientation on the environment and how it would be augmented by an intelligent environment.

The user study began with discussion questions in order to orient users on the nature of the invisibility problem and intelligent environments. Participants then used the MVI to examine the personalisation process and answered questions on their privacy and information sharing within this intelligent environment. An example interface screenshot from the study is described in Figure 9. The services available to the users of this study included information on environmental conditions and resources (e.g. air conditioning, nearby printers, environmental Bluetooth sensors), provided directions to users (e.g. campus-wide or locally within the building), and gave access to news and ‘find-a-friend’ locating services.
Chapter Four: Preliminary Investigations into Privacy in Intelligent Environments

MyPlace Visualisation Server

- **Location:** N44 - Building Foyer [view]
- **User:** Identified Logout

You are connected to an external location server. You have 0 friends nearby.

**Devices**

At this location:

- **Air Conditioning** Air conditioning controls. [link]
- **Printer** Find the nearest accessible printer... [location]
- **Sensors** Bluetooth sensors, microphones, and video cameras capture information for making the room smart. Lighting sensors for energy conservation. [info]
- **School Information Centre** Access the school's subject database. [subjects]
  [homepage]

**Locations**

Nearby this location:

- **Campus Map** University Campus map. [locate this building] [general map]
- **Postgraduate Workspace** Location of ICT Postgraduate Workspace [location]

**Services**

Available at this location:

- **Wireless Networking** [Wireless]
- **News Updates** - [www.news.com.au]
- **Location Server** - Configure location sharing options. [configure]

![Load Default Personal Attributes](load_default.png)

Figure 9: MyPlace Visualisation Server Screenshot

The necessity to create and in some cases fake environmental services in this study, and the fact that users were only given one interaction opportunity, meant that users did not have the chance to use the services throughout their day, potentially limiting their ability to accurately judge the usefulness of the services. The questions asked during the experiment also challenged users to consider long-term problems that may not have been immediately evident but would have impacted on the user in the long term. The fact that we were providing realistic services in the student’s natural environment did boost the external validity of the results. Users were reacting to services that could have assisted them in their daily activities. The selection of early adopters of mobile technologies, and therefore the likely early adopters of these services, also adds to the study’s external validity. The results from this users study are therefore useful in considering how users would like to interact with ubiquitous computing services and its supporting infrastructure.

Participants were recruited by requesting volunteers around the university campus where the study took place. Seventeen users took part in this study, comprising eight males and nine females. Most participants were in their twenties (12 users), reported their field as ‘IT’ (12 users) and owned a mobile phone or PDA (14 users). This population is not representative of all future users of intelligent environments, which was impossible due to the resources available to this project. These users do however provide an insight into the
privacy and identity concerns users have when interacting with intelligent environments. Again this user study is part of the larger validation of our results through multiple-user studies and by comparing our results with existing research.

4.5.2 User Study Results

To identify the effectiveness of using the above interface to explain the difficulties of displaying relevant information within an intelligent environment, we asked users to describe the invisibility problem and the process of personalisation. While four users professed not to understand the invisibility problem, the others described it as a form of personalisation and identification of relevant intelligent environment services. All users seemed happy with the descriptions of these processes given during the pre-study discussion questions, and the authors feel that users understand the need for this type of invisibility and personalisation.

User feedback on the MVI included concerns about the navigation and presentation of such a large amount of information on such a small screen, including the need for a more graphical interface to better organise information, and the desire to have more effective personalisation of the displayed services. Fifteen participants (88.2%) indicated that they considered the services to be useful, while the remaining two users described other location-based services they would prefer to see in this intelligent environment. Other users’ comments indicated that the delivery of these services could be better customised to their needs or that ‘only anonymous services would be useful’.

Users were asked to rate, on a scale from 1 (not) to 5 (very), how concerned they were with the collection of either generic user information (e.g. whether a student or staff member, interests, etc.) or more identifiable information (e.g. name or ID number). As expected, users showed a low level of concern (2.00) in sharing generic information with the environment, but were much more concerned (3.41) with sharing personal information. Twelve users (70.6%) indicated that they would be more likely to share more personal information if the environment were unable to link this information to their real identity. All other participants indicated that it would not affect their information sharing preferences, with user comments describing their wish to see ‘tangible benefits’ before sharing personal information. This reinforces the already identified desire of users for anonymous environmental interaction.

Users were then asked whether the ability of the intelligent environment to further share their information outside of this environment would make them more or less likely to provide personal information to personalise their interaction with the intelligent environment. Ten users (58.8%) noted they would be less likely, with half of these users citing the potential for abuse as their reason. Five users indicated that it would have no effect, while two participants declined to answer, commenting that it would completely depend on what information was shared with what intelligent environment. The final survey question also addressed this topic. It asked if any personal information were restricted to use within the environment it was shared with, would the
user be more or less likely to share personal information. A similar result was found, with nine users (52.9%) indicating this would make them more likely to share information. These results support the view that information should be prevented from flowing across an environment’s boundaries to reduce risks to users’ privacy (Langheinrich, 2002).

Users were then asked to consider the use of a centralised location service that provided users’ name and location details to other users, in accordance with their personal preferences. User responses on the likelihood of using this service showed reluctance, the average being 2.76, with the only user responding with a ‘5’ commenting that the university setting gave them some trust in the intelligent environment. When asked whether the restriction of access to the user’s current location (i.e. historical searches were not allowed) would make them more or less likely to use this service, eleven users (64.7%) responded with ‘more likely’ and six users (35.3%) remained unchanged. Thirteen users (76.5%) identified that control over who could have access to their location information would make them more likely to share this information. Users are more comfortable sharing information when they can actively manage risks to their privacy.

To further investigate information-sharing preferences, users were asked to describe who they would normally share their location information with. Most participants indicated that their friends (15 users, 88.2%) or co-workers (11 users, 64.7%) were the only people they would share this information with, and several user comments indicated that more fine-grained control was needed (e.g. only sharing location data with colleagues during work hours). Only two users indicated that they would share information with all users or with commercial services and only one indicated that he/she would allow the sharing of his/her location history.

This result was reflected when participants were asked to consider the sharing of all information. Fourteen users (82.4% of all participants) agreed that the ability to control who has access to their information would make them more likely to provide information for the personalisation of intelligent environment services. 76.5% of users also indicated that knowledge of the owner of an intelligent environment would affect how much information they would share, and many users commented that this was related to their trust of the intelligent environment’s owners.

4.5.3 Discussion and Design Conclusions

Personalised information access has been given very little attention in ubiquitous computing research. This is unfortunate because it is an important method of overcoming the information invisibility that occurs within intelligent environments. In many of these environments, there will be a real need to personalise communication to match the user’s knowledge, especially their familiarity with the intelligent environment and the services within it. Equally, intelligent environments offer a potentially important context for personalisation research because intelligent environments can use evidence collected about users within an intelligent environment to build user models and to deliver personalised services.
Chapter Four: Preliminary Investigations into Privacy in Intelligent Environments

The results of this user study show that users are concerned about their privacy and want to control the flow of their information. Users want control over who has access to their information and want explicit feedback on the use and distribution of this information. When users evaluate a specific information exchange, they are evaluating their trust of the system and the expected tangible benefits they receive for providing information. Intelligent environments should seek to make feedback on the information as complete as possible to allow users to make their own determination of the risk to their privacy versus the perceived reward for sharing information.

Intelligent environments must be designed to provide users with enough information to understand the impacts of sharing information and to weigh the risks to their privacy with the potential benefits of any available services. The flow of information across physical, temporal and social borders (Langheinrich, 2002) should be controlled by the users where possible to reduce unforeseen risks to their privacy. The design of any intelligent environments should also examine methods of promoting and/or managing users’ trust and reputation. Users in this study demonstrated that they understood the invisibility problem and were willing to provide personal information in exchange for effective personalisation. Effective management of this balancing act of providing valuable services without breaching users’ privacy will determine whether an intelligent environment is accepted and utilised in everyday environments. These requirements are integrated into chapter five when designing the required characteristics of the dissertation’s ubiquitous computing infrastructure.

4.6 Summary and Conclusions

This chapter has highlighted the exploratory research conducted to better understand users' interaction with intelligent environments and ubiquitous computing technologies. Overall this research has observed much trepidation amongst users about the potential for privacy abuse by the information collection and reuse within intelligent environments. Users expressed clear preferences for maintaining control over any exchanges of information with the environment, and highlighted the need for feedback on how collected information should be used and who can have access to it after its initial collection. When sharing information, users highlighted the importance of establishing if any prior relationships with the intended third party existed, and such a history represents a very important context for users when determining the effect of an exchange of information on their privacy.

This chapter's modelling of user interaction within an intelligent environment demonstrated the need for personalisation of the users' interaction interface. The need to personalise any interaction without providing the intelligent environment with the user's interaction history (or their interaction preferences), and thus breaching their privacy, requires the use of user personae and the personalisation of the intelligent environment’s service or user interaction interface on the user’s mobile device. This increases the amount of data required to be sent to the user’s device, potentially causing bandwidth problems when using older or less computationally impressive
mobile devices or crowded wireless networks. However, this reduces information flowing from the data owners to the data collectors, which is a key requirement in improving users’ privacy (Jiang, Hong & Landay, 2002).

An initial intelligent environment architecture was developed to reflect the privacy design requirements detailed in section 2.4. The initial design requires third-party confirmation of identity, the use of permanent, user-maintained, Internet-accessible entities to serve user information requests and manage global ubiquitous computing services, and the separation of the environment’s user register and service providers to prevent unapproved information reuse between entities. The architecture provides users with anonymous interaction with the environment, whilst still providing easy to use identity authentication for partial or complete user personae. Further development is required to investigate what information would be exchanged when connecting with an environment, and to consider the impact that these exchanges would have on user privacy.

The final user study further highlighted the need for user control of information exchanges, the use of personae to conditionally represent the user in a particular context, and the need for anonymous interaction with the environment. Users particularly need enough information about an information exchange to effectively judge its impact on their privacy. This includes feedback on the environment’s owners, its information collection and reuse, and any available information on the trustworthiness (or reputation) of an entity or service. These suggestions are considered when developing the final intelligent environment architecture described in chapter six.

This research underscores the importance of users having control of their own information, including the selection of interaction personae, and the need for a flexible architecture that is service independent. This suggests the necessity for a ubiquitous computing infrastructure comprised of the generic intelligent environment architecture, and this could be used to provide interaction consistency between different ubiquitous computing environments. The design of this ubiquitous computing infrastructure and its impact on the design of the generic intelligent environment architecture that underpins it is examined in chapter five.
Chapter Five: Privacy Requirements for Ubiquitous Computing Systems

5.1 Introduction
Intelligent environments seek to provide services to users within physical environments with ubiquitous computing resources. It has been suggested that these environments will soon be in our homes, offices, cars, schools, hospitals, aged care facilities and anywhere where there are large groups of people, such as in shopping malls and on public transport. Services that have been suggested for these environments range from physical location trackers, to identifying close-by friends, providing local environmental information and managing environmental conditions (like temperature) based upon the user preferences. These types of systems have thus far been designed to work in isolation, with existing systems primarily developed to prove new technologies or to investigate an aspect of information sharing amongst members of a particular group.

Ubiquitous computing research therefore lacks a holistic view of the information flow required if intelligent environments are to support more than isolated pockets of our world. The dissertation seeks to identify how these environments can seamlessly work together in a way that maintains user privacy and information security, yet still allows personalised services to support people as they go about their daily lives. To do that we need an understanding of the types of ubiquitous computing environments that we are developing and how these environments will form part of a greater infrastructure. This chapter defines the technical and interaction requirements for this ubiquitous computing infrastructure, and combines these into the requirements for this research’s intelligent environment architecture.

5.2 Ubiquitous Computing Infrastructure
Successful ubiquitous computing applications tend to result from computing support for pre-existing valued interactions (Stringer, Halloran, Hornecker and Fitzpatrick, 2005). An architecture that hopes to be successful in common everyday environments needs to provide additional, valuable support to existing environmental interactions. These environments need to provide additional services without endangering user privacy, and to allow the same types of interactions and existence that existed without the intelligent environment, e.g. allow anonymous interaction and existence with the space. To accomplish this level of interaction, we need to ensure that the intelligent environment allows users the same interaction and control of their personal data and privacy risks that they have in more traditional non-computer based interactions.

The dissertation’s goal, seen through the lens of Activity Theory, remains the identification of an interaction environment that supports users’ ability to
interact with services in a private and secure manner. But to accomplish this level of understanding, the dissertation needs to consider the broader picture regarding the interactions and supporting entities that are required. User studies were used (see chapter four) to better understand users’ interaction requirements. The community’s use of identity authentication tools and social and technical mechanisms to secure their user devices were also examined. These influences must be considered when developing the tools with which users will make these service interactions.

The Critical Heurists approach (Ulrich, 1987) requires the examination of everything in the research environment that is not fully understood. Whilst the technical protocols and structures of ubiquitous computing environments are generally understood, less is known about the types of interactions required and how these motivations impact on the required tools which need to be in the environment. The analysis of the dissertation’s required boundary justifications highlights in particular the need to consider user interactions with multiple intelligent environments, the types of service interactions required, and consequently the types of infrastructure that would allow these multiple varied interactions.

Intelligent environment architectures must have an infrastructure that allows users secure and private management of their identity and interactions with the environment. The collection, storage and use of all information within the intelligent environment must be managed to allow the use of information by the environment to provide personalised services whilst maintaining user privacy. The communication networks for exchanging information and interacting with the intelligent environment must be secured to ensure user privacy and prevent collection of user information and identity theft. And finally the intelligent environment must use consistent interfaces that can provide the user with the information they require to understand and improve their interactions with the environment.

When considering the required characteristics of an intelligent environment, it is important to consider what intelligent environments would be used for and what structures they would need to accomplish these goals. Intelligent environments are embedded ubiquitous computing environments that provide personalised services to users via their mobile device or public interfaces. This section seeks to define the requirements for an infrastructure to support these environments and to provide the global entities necessary for their integration across multiple areas of our everyday lives. It considers the role of ubiquitous computing environments in creating digital interaction spaces for greater community connectedness and user interaction; examines the identity providers required to authenticate user’s identity within the environments; examines the storage and security of user information; and considers potential interfaces to interact with a ubiquitous computing infrastructure.

5.2.1 Digital Communities

Numerous digital communities currently exist across the Internet (for examples refer to section 2.2.3). However, these digital communities do not provide the community connectedness that Oldenburg (1999) suggests is
missing from modern cities. They provide no tangible sense of presence or connection to the user’s local community. Furthermore, their access is limited to people with Internet access, and there are often complex social hierarchies at work, preventing a relaxed ‘social levelling’ atmosphere from evolving. This section examines the development and support of digital communities using our ubiquitous computing infrastructure.

5.2.1.1 Privacy within Ubiquitous Computing Environments

Privacy is of considerable concern within ubiquitous computing environments due to the pervasive capture and reuse of personal information which can lead to incredibly accurate profiles of their user’s personal attributes and preferences. This concern comes at a time of increasing identity theft and fraud, and this continues the increasing distrust by the community and the need for reclusive privacy identified by Oldenburg (1999) as our communities continue to move more towards isolationist tendencies. ‘A facilitating public etiquette consisting of rituals necessary to the meeting, greeting, and enjoyment of strangers is not much in evidence in the United States. It is replaced by a set of strategies designed to avoid contact with people in public, by devices intended to preserve the individual’s circle of privacy against any stranger that might violate it.’ (Oldenburg, 1999, p. 13)

User privacy is not, however, the exclusion of information sharing with others; it is in fact the ability of an individual or group to determine themselves when, how and to what extent information about them is communicated to others (Westin, 1967). Users need enough information to judge the impact of an information exchange on their privacy, and they want anonymous interaction possibilities when not exchanging information for something of perceived value (i.e. a service). The observed willingness of users to give up information (for any perceived benefit) despite their stated privacy preferences suggests that a minimum level of privacy should be integrated into any intelligent environment’s architecture. These privacy minimums should be determined by users’ privacy perceptions and by the most restrictive privacy laws that will cover the environments that the intelligent environment will be placed within.

To allow social forces to shape the use of the environments, and the privacy of their users, we suggest the use of a flexible system that allows users to mimic the interactions of their non-digital lives. Users should be able to determine what information is used to represent them, interact with services and other users anonymously and dynamically determine what information can be shared when interacting with the environment. These protections (coupled with adequate security) allow users to interact privately with intelligent environments until they have something to gain from an information exchange (i.e. a service). In this way users are able to weigh the benefits of using an intelligent environment versus the risks to their privacy and choose whether to interact with an environment based upon those determinations.

Chapter four highlights the need for anonymous environmental interaction, control of user persona usage and information exchanges, prevention of information flowing across natural borders of privacy, and the use of
Chapter Five: Privacy Requirements for Ubiquitous Computing Systems

reputation or trust systems to provide additional context for an information exchange. These results mirror existing research that has found that users want control over any information sharing (Iachello et al., 2005; Nguyen & Mynatt, 2002) and the privacy policies applied to any collected information (Nguyen & Mynatt, 2002), and want collected information’s use to be limited to the current environment (Langheinrich, 2002). Information sharing between community members can be facilitated as long as users have appropriate control and feedback on information gathering and use within the environment. The potential benefits derived from the ‘third places’ hosted by these digital communities greatly exceed the potential damage to users’ privacy, particularly when our generic privacy design recommendations are integrated into the architecture.

5.2.1.2 Interaction Design Requirements

The intelligent environment architecture could be used to provide a variety of services that could promote community interaction through the creation and support of (virtual and real) third places. But the integration of digital communities into the ubiquitous computing infrastructure is about more than user privacy or an individual community forum’s usability. Of particular concern is how the use of the ubiquitous computing technologies to deliver ‘third places’ affects their effectiveness. This section investigates these services, particularly considering the impact of ubiquitous computing on the localisation, accessibility and presence of virtual third places.

The use of ubiquitous computing systems addresses some of the primary concerns of creating ‘virtual third places’ simply due to their contextualisation in a physical space. Intelligent environments cover a particular physical location, and any ‘virtual third community’ would normally be accessed from within that community. This localises the virtual community in the ‘real’ community, and this localisation provides the users with an actual sense of ‘presence’. Users would actually be in the environment whilst interacting (either synchronously or asynchronously) with other community members.

These ubiquitous computing environments are accessed using mobile phones or other handheld computing devices (e.g. PDAs) from within the physical environment. Data transfers throughout the environment should be limited, and encryption should be standard for all communications. The potentially limited computational power of the interaction devices should not be seen as endorsing the use of weaker encryption regimes though, as it would be easy for a malicious entity to mine information from within an environment with the intention of decrypting it later on a supercomputer.

External access could be restricted depending on the purpose of the environment, but this would increase accessibility, and the fact that most users would be physically situated within the environment would heighten its relevance to the local community. This ease of access and openness to all users should promote the ‘social levelling’ experienced in physical ‘third places’. This would also require users to have complete control over the sharing of their identity and should allow anonymous or avatar-based interaction to promote the sense of playfulness and accessibility.
A ubiquitous computing infrastructure could support community interaction by hosting existing virtual community structures. Discussion boards, chat rooms and multi-user domains (MUDs) could all be used for (localised) virtual community interaction and to promote interaction in real third places. Environmental services could provide local directions, background and information on community group meetings. For example, environmental services could identify local meeting places, provide local background information to foster a better sense of community and identify regular (formal and informal) meetings of groups and associations. A further (optional) service might provide public information on the environment’s occupants, which could promote better community interaction by reducing barriers to interaction with strangers. This will only be successful if users have complete control over their public information or the ‘face’ (Lederer, Dey & Mankoff, 2002) that they present to the environment.

Supporting users’ interaction amongst their urban tribes requires us to look past existing communication and awareness tools like Instant Messenger (IM), Voice over IP (VoIP) telephony software and email. Whilst these tools will be useful and accessible via the ubiquitous computing infrastructure’s Internet access, ubiquitous computing services will allow more effective communication with the entire group. Ubiquitous computing services can locate nearby friends, coordinate calendars or schedules and provide awareness of a group’s activities. These tools require access to a central server, most likely via the Internet. Providing Internet access through the environment would add further value to any such environment and assist in building user acceptance of the infrastructure.

5.2.1.3 Community Interaction

A ubiquitous computing infrastructure could be utilised to promote a greater integration of the community and more effective use of virtual and real third places. We suggest that cities could be covered in city-wide wireless computing networks that form the basis for a ubiquitous computing support infrastructure providing support to the local community. Ubiquitous computing services could provide local information, enhance community coordination and provide virtual third places for interactions by community members. By using ubiquitous computing environments to host and access these virtual communities we overcome some of the shortcomings of accessing virtual communities using more traditional computing devices.

Central to the privacy requirements of using ubiquitous computing environments is users’ explicit control over their information’s use and distribution. The standard information (or public profile) provided to the intelligent environment should be descriptive, non-unique and designed to engage with other members of the community. Contact information could easily be integrated into this system, but should be sharable only with the explicit consent of the user. To be more secure, this exchange could occur locally without involving the intelligent environment’s network (e.g. via Bluetooth or infrared). It is hoped that the user interface will take some steps
to address the anonymous nature of crowds in our larger cities and reduce
the barriers to interacting with strangers observed by Oldenburg (1999).

If this community’s interaction interface is to be successful, it must be widely
available, and must be easy to use and valuable for its users. The increasing
costs and ultimately exclusive nature of commercial systems suggests a
publicly funded or not-for-profit model would be more effective at supporting
and creating the essential elements of successful third places. Ubiquitous
computing services that add value to the infrastructure (e.g. local information
access, Internet access etc.) will further increase the community’s interest
and engagement in the infrastructure and promote its success. Conversely,
fee-based or service-poor systems would discourage participation and make
the infrastructure less effective.

5.2.1.4 Usage Scenario

To provide a more grounded discussion on this infrastructure, let us consider
a hypothetical intelligent environment proposed for the Kangaroo Point cliffs
area of Brisbane, Australia. The site of an old quarry along the Brisbane River,
this area provides recreational rock climbing, boating and sporting facilities
to the general public. A social area used by many as a third place, this
environment could benefit from a ubiquitous computing infrastructure to
provide local information, highlight local activities and climbing group
meetings and provide more traditional ubiquitous computing services. An
interface to access the environment’s services would allow users to access
their personal network (or urban tribe) via group communication and
awareness tools, see and manage their shared identity, utilise the intelligent
environment’s services (e.g. accessing a community discussion board or
commercial service) or receive information on the local area.

Consider the following scenario of using the suggested user interface (refer to
Figure 10) to explore the area and interact with the local community.

```
Kangaroo Point Cliffs - Brisbane, Australia
Brisbane City Council BCC-021

Contacts | Services | Local Area

Cameron
Details:
Live in New Farm; http://www.cameron.org

Melissa
Details:
Attending Griffith Uni. 21. Theatre Student

Wingman07
Details:
Play Rugby for Sunnybank Dragons.

<Filter Display>
<Search for User>

Belinda
Details:
East Brisbane ...

<Location>
<More Details>

<Exit>
```

*Figure 10: 'Local Area' User Interface Screen*
Belinda has recently moved to Brisbane to start university and is exploring the city. When Belinda enters the environment, the 'Local Area' screen shows her all users logged into the environment with a 'public face' selected. If Belinda chooses, she could also select to remain anonymous, but hoping to meet new people she selects her usual profile describing her and providing a picture. If there were lots of users in the area, she could filter the users to show only people that met some specified criteria (e.g. users over 20). Walking along the base of the cliffs and noticing a climber that matches a user profile’s picture, Belinda approaches him and strikes up a conversation.

When connecting to the environment, her PDA connects her to her social network which updates her location on its server and returns a list of all her friends currently connected to the service. A few minutes later a warning beep informs her that a friend has just entered the nearby area, and she sends them an instant message to see if they want to meet up. Belinda’s friend suggests they meet at the boathouse, and not knowing where this is, she selects ‘more details’ on the local area screen. This prompts the systems to display a map, some local information and a short history of the area. As she finds the boathouse, Belinda notices in the local information that a climbing group meet regularly at the cliffs, and she makes a note to join them the next time she’s available.

Belinda could use the ‘Services’ tab to access the services provided in this intelligent environment (refer to Figure 11). Each service is displayed with links to relevant information and any available interaction and personalisation histories. Selecting a service loads the interface maintained by the service provider, using the identity set using the ‘ID Manager’ interface. Services could be colour-coded in this interface so users can identify different service types at a glance.

![Figure 11: 'Services' User Interface Screen](image-url)
This interface demonstrates the types of interactions a user is likely to have with an intelligent environment, namely interaction with environmental services and other users, access to local information and communication with the users’ friends and family (i.e. their ‘tribe’) via global services.

5.2.1.5 Discussion and Design Conclusions

This ubiquitous computing infrastructure has the dual purpose of supporting community interaction in real third places, whilst providing hosting for localised virtual communities that form virtual third places. Community interaction is supported by providing a new interface to promote interaction with people in the local area. Traditional and ubiquitous computing communication and awareness tools can profitably be utilised to allow micro-communication and the coordination of meetings amongst existing social groups. The development of community interaction spaces using ubiquitous computing environments should ultimately allow the evaluation of the effect of third places on community spaces and an investigation into how successfully they can be created using ubiquitous computing environments.

Our scenario briefly describes the interaction that occurs when a user enters the environment and accesses the ubiquitous computing infrastructure. Users select a ‘public face’ that they wish to share with the environment, and this is passed to a central server to be shared with other users. The demographic information contained in the profile can then be used to personalise users’ display of the environment’s other users. However, the exchange of this information, and the user’s personalisation preferences, can prompt privacy concerns amongst users.

To avoid sharing excessive amounts of information with the environment, the personalisation of the user display occurs on the user’s handheld device. The demographic information provided to the environment (to facilitate sorting) should be sufficiently vague to prevent the recognising of the user across multiple (and potentially environmentally distributed) ubiquitous computing environments. To further prevent user tracking, the public profiles selected by the user should not be stored in the environment or be linked to any ubiquitous computing service usage. This provides an anonymous infrastructure that users can use without fear of being tracked or of detailed profiles of the users’ activities becoming available to third parties. These environments will also be less effective if other privacy invasive or socially unpopular services are forced upon the user (e.g. directed marketing or pop-up advertisements), as these would turn people off interacting with the infrastructure.

Virtual communities provide neutral places away from work and home that allow playful conversation and interaction. But virtual communities are often frequented by a very specific user group and lack the ability to promote interaction across a diverse community population. By providing access to these environments via ubiquitous computing, we effectively ground the virtual communities in real-world environments and provide easy access to the greater community population. The benefits of this can be examined by
contrasting traditional and ubiquitous computing access to virtual communities.

A virtual community set up to provide discussion on local issues is only effective as a third place if it examines local issues and if it is accessed by a wide range of community members. Virtual communities therefore need to advertise their existence to community members, must be easy to access (and visited regularly) and must promote casual conversation that is free from politics or power. Traditional virtual communities have access problems, owing to the varying levels of computer literacy and access to the Internet amongst community users. Virtual communities’ lack of localisation often reduces their relevance to the community and leads to unique knowledge-based power structures not conducive to relaxed, playful interaction.

Virtual third places served from our ubiquitous computing infrastructure are accessed via common handheld devices. The existence of the intelligent environment is immediately obvious to anyone entering the environment, and this localised access ensures the entire communities have the opportunity to interact with these virtual third places. Furthermore, this localisation allows the rich context of the physical environment to interact with the virtual third place, and this promotes the sense of presence of these environments. Finally, the anonymous interaction possibilities can lead to a sense of playfulness and casualness in the interactions that occur in these places. These factors make the virtual third place more accessible and relevant to the local community if served by a ubiquitous computing environment.

5.2.2 Ubiquitous Computing Services

An intelligent environment’s services have been classified by either the information used to deliver them (e.g. Historical or Real-time) or by the interaction mechanisms they use (e.g. ‘interrupt’ or ‘query-based’ services) (Price, Adam & Nuseibeh, 2005). But these classifications ignore the role of the service deliverer in the greater ubiquitous computing infrastructure. Users of an environment may well want to access services from another location or environment. Interaction with these services might require specific privacy or security safeguards to ensure the user’s privacy is protected. This section takes into account the needs of a scalable, accessible ubiquitous computing infrastructure in integrating intelligent environments and their services into users’ everyday lives.

Mobile devices are currently available with mobile web browsers and advanced multimedia capabilities that could be utilised to interact with an environment’s services. Specialised (and more complex) services might require more direct service delivery using local server delivered content. These services may adopt tools similar to the service aggregators used in the iCrafter Service Framework (Ponnekanti et al., 2001) described in section 2.3.2.7. In either case the environment must provide a locator that advertises the access point (e.g. a local network address) for service. Service advertisers should not require any user intervention or information to obtain the access location, and must include enough information to allow users to determine whether they wish to use a service.
The use of aggregators in delivery services have their advantages, primarily in providing users with familiar interaction interfaces and the ability to adapt to new environmental services. The ability of the aggregators also to combine multiple services to achieve larger goals will be key in providing value from a ubiquitous computing environment. But this centralised view of service delivery has risks to users’ privacy. If all services are requested from one source, then it could develop a detailed user profile that could be saved or revealed to a third party. This suggests that, where possible, services should be delivered from separate providers.

The sheer variety of services that could be delivered through intelligent environments suggests that our infrastructure must be service independent. Users should also be able to interact with an intelligent environment without providing personal information, and wherever possible services should be usable anonymously. Many services are global and require access to external databases or third parties, e.g. commercial, information access or communication services. Other services are environmentally based, either requiring interaction with a local service provider, for example local information delivery, resource discovery or community interaction services, or possibly physical interaction with their environment, for example using a public touch screen.

Global services are interesting to consider, because they have specific design requirements that must be incorporated into a ubiquitous computing infrastructure. Global services by definition suggest that intelligent environments must provide users with Internet access for direct access to these services. Indirect access to these services via an intelligent environment has significant privacy concerns, as it reduces the visibility of information provided to the global service. The collection of data in one environment and its transmission to another breaches fundamental privacy principles (Langheinrich, 2002), but the decoupling of global services from local environments would reduce the expectation that information will stay within a particular physical boundary. Global services would not therefore be advertised at a local level in the same manner as environmental services.

Environmental services are those that service a local environment (potentially personalising service delivery based upon the local contextual conditions). Environmental services should maintain a local focus and not pass information outside of the environment without explicit user consent. The advertising of these services should be done in a way that restricts their access to users within the environment. Environmental services that require external identity authentication are not considered global services, but these do require Internet access to contact the user’s identity broker. Examples of both environmental and global services are described in Table 13.

<table>
<thead>
<tr>
<th>Environmental Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commercial:</strong> Delivery of goods and services</td>
</tr>
<tr>
<td><strong>Interactive:</strong> Manipulation of the environment or artefacts (e.g. ambient devices, multi-modal interaction)</td>
</tr>
<tr>
<td><strong>Resource Discovery:</strong> Users’ availability and computing resources discovery (e.g. available printers or interaction devices)</td>
</tr>
</tbody>
</table>
Local Information Delivery: Access to environmental information (e.g. notices, maps, advertising)

Community Interaction: Users’ interaction and community message boards (e.g. blogs, notice boards, feedback forums etc.)

Sensing: Environmental security and user adaptive services

<table>
<thead>
<tr>
<th>Global Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Access: Internet (e.g. Google search, news aggregators) and database access (e.g. ACM Library)</td>
</tr>
<tr>
<td>Communication Services: VoIP and instant messenger services (e.g. Skype, MSN, etc.)</td>
</tr>
<tr>
<td>Personal Services: Third-party services accessed via Personal Domain (e.g. organizing calendar, friends locating service etc.)</td>
</tr>
</tbody>
</table>

Table 13: Examples of Intelligent Environment Services

This list of services is unlikely to be exhaustive. New services and delivery methods are almost assured as users and merchants find different ways of advertising their availability or goods. One possible extension is the use of these environments by users to advertise their services or assistance. For example a user might use the environment to offer emergency first aid or justice of the peace services, or a coffee-cart retailer could advertise their products and the times they were available. Service delivery is ultimately likely to change also, as users make use of greater capacity mobile devices or through the design of simpler recognition systems using biometrics or simple beacon-like devices (e.g. a RFID-enabled watch). The privacy and security concerns of using simpler user interfaces are outside the scope of this research, but they are discussed in section 8.3.1. Biometrics is discussed in section 8.3.5.

5.2.3 Identity Management

To be truly useful, intelligent environments must support the plurality of identities that users can use in the physical world. Users must be able to prove they have access to services that may be restricted by age – like buying a movie ticket, or identity – such as keyless access to your home or car, without requiring identity confirmation for anonymous or unrestricted services. Users must be able to wander anonymously between different environments and use services without needing to prove their identity. In this manner we are recreating the familiar safe and trustworthy interactions with our communities whilst reducing the dangers from any individual or group of intelligent environments to the user’s privacy.

Users must be able to recreate the different identities that we use when interacting with different groups. People represent themselves very differently depending on their current context (current motivations and morality) and audience, and may want to be represented equally differently within separate intelligent environments. Each ‘identity’ or pseudonym could contain a different subset of the user’s information tailored for a specific purpose or location, for example, financial, medical or postal information, or it could contain preferences for interacting with a specific environment. Furthermore,
a user may only want to share their identity with specific services or other users of the environment and remain anonymous to the intelligent environment itself.

Users need to be able to verify their identity in different ways depending on their goals for interacting with the environment. Users must be able to assert specific personal information without providing the intelligent environment or services providers with their complete information. Users must also be able to privately share information with other users depending on their identity, their own willingness to exchange information, and the information they request. There is also support for the use of signed pseudonyms (or templates) (Hitchens, Kay & Kummerfeld, 2004) that users can reuse when interacting with a particular intelligent environment or type of service. These signed pseudonyms allow environments to have some confidence in user-supplied information without requiring an arduous identity confirmation process.

This view of identity management requires that users be able to create, alter and switch between multiple personal identities for interacting with an intelligent environment, and that services have some method of confirming the authenticity of a user’s identity using a trusted third party. This requires a secure method of interaction to allow sharing of identities without risks of collusion between environments or identity theft, and should allow parts of a user’s identity to be confirmed without requiring access to the whole of their information. Finally, this framework must be generic enough to provide support for users across multiple (and potentially vastly different) intelligent environments, yet specific enough to provide security and peace of mind for users, and guidance for intelligent environment developers. The impact of these requirements on our infrastructure is investigated in section 5.3.2.

Examples of global identity management entities include the Liberty Alliance framework (Liberty Alliance, 2002), Shibboleth (Shibboleth, 2005) and the OpenID architecture (Recordon & Reed, 2006). The Liberty Alliance framework was a federated identity system that provided single sign-on identity management. It does not allow for users to choose what identity they wish to use in a given context. Sibboleth and OpenID allow this fine grain control by authenticating limited identity personae. The more identity providers that are available for authenticating user’s identity or attribute assertions, the greater confidence the service providers can have in these assertions.

More effective ubiquitous computing architectures will provide a number of identity authentication options for users to utilise. As use of the identity providers grows these projects will reinforce each other and become more acceptable as methods of identification. An intelligent environment should work with any identity manager to prevent the architecture from being tied to a particular interface or notation, and to allow intelligent environments and users to use the most relevant and trusted identity providers. For example, Australian users might use a local identity manager whilst within Australia, but use an international identity manager for interactions elsewhere.
Payments within intelligent environments for services are likely to use existing traditional electronic payment systems in the same way as they do in the real world. However, these payments do not normally provide users with any anonymity, and thus could be used to track users’ activities within an intelligent environment. Anonymous forms of payment that act like cash in the physical world would be preferred. E-Cash (Schoenmakers, 1998) (based upon the earlier ‘Digicash’ and its use of blind signatures (Chaum, 1983)) provides an anonymous method of paying merchants and other third parties. CybaCard (http://www.cybacom.com/) is an anonymous Mastercard account that can be used online, with purchases charged to a normal payment card. For more information on anonymous transaction systems see (Claessens, Preneely & Vandewalle, 1999).

Other interesting payment schemes include the use of micro-payments within intelligent environments. Micro-payments are very small payments made electronically for access to services, webpages or other electronic resources. Micro-payments cover transactions that are too small to be economical as credit card transactions, and can be as little as a fraction of a cent. They could be used within intelligent environments as payment for services or as a charge for accessing a user’s personal information (to prevent malicious programs or environments from trawling for user information to build user profiles). Although many micro-payment schemes have been developed, there has been limited adoption by financial institutions or in the wider community.

The dissertation’s architecture will not mandate methods of payment between users and services due the multitude of payment methods and potential service types. The types of payment methods adopted by users are also likely to be regionally specific, integrating with the users’ existing financial institutions and any applicable local legislation. Users will have to consider the effect of making identifiable purchases on their preferred level of privacy when interacting with an intelligent environment.

5.2.4 User Interaction

The interactions that a user will have with an intelligent environment are predominantly determined by the services on offer and the information that the user will need to provide to access the service, versus the benefits the user would expect to obtain. Users can also access an intelligent environment to interact with other users. The architecture to be developed in the dissertation must therefore provide a secure and private method of identifying available services and users. This must include a framework to exchange information to allow users to determine the benefits or risks of interacting with the intelligent environment.

The user studies in chapter four examine the information needed to make these judgements. Users want access to information describing the owners of the service and their information collection and privacy policies, and users want to control information shared with services. Prior relationships with service providers or other users are especially important, and these should be readily available from the user’s interaction interface. The results also validate other research calling for the use of trust and reputation systems and the
need for explicit feedback on information collection and usage activities to improve users’ ability to judge the privacy risks of interacting with a service.

The type of interaction required (either query or interruption based) and data used in a service (either historical or real-time data) also impacts on how a service can be accessed and what information the service requires. Each of these cases must be addressed in any architecture. An intelligent environment must provide a secure method of communicating with service providers, and information exchanged with the services must be stored securely; stored information must not cross natural borders of personal privacy or breach any other fundamental privacy design imperatives (see section 2.4).

A ubiquitous computing infrastructure should utilise a method of privately discovering and accessing available environments and services on the user’s mobile device. This occurs on the user’s device to prevent their interaction preferences from being mined by any environment they interact with. Service usage must be user initiated, and information shared only when expressly approved by the user or their information sharing preferences. Anonymous interaction with services should be encouraged, but, conversely, relevant users should also be able to provide any relevant contextual information to improve service delivery.

Intelligent environments are typically served directly to users’ mobile devices. If a user enters a space covered by an intelligent environment without a mobile device, they will normally have no access to the environment’s services. Environments that have particularly useful services should provide a public interface for service interaction. Environments that use sensing technologies should also have non-digital notifications (such as a discreet sign) that highlight this surveillance to the general public. Interaction between users within an intelligent environment is also required, but this interaction must be opt-in. Users would therefore have to connect to the intelligent environment and indicate through direct confirmation or privacy preferences that they wish to be visible to other users for interaction purposes.

Services can be administered remotely (via the Internet) or directly (to a user within the local area). The physically present nature of any ubiquitous computing devices provides additional possibilities for interacting with hardware (via touching components or using short-range transmission technologies like infrared or bluetooth). The types of services available within an intelligent environment will determine the range of necessary interactions. This means that, in order to develop a generic intelligent environment architecture, we need to identify the types of services that may be available and identify all structures required to support these services.

Interaction with services should follow accepted strategies that reduce the impact on user privacy. Services should allow interaction with a minimum of user information, and this information should be proportional to the benefit provided. Furthermore, any information provided to an environment should only be used as part of clear information reuse policies, and should only be used in other environments with the user’s express permission. Lastly, information exchanges should, where possible, have information
predominantly flowing to the user, and feedback about the exchanges must provide the user with enough information to accurately judge the risk to the user's privacy.

5.2.4.1 Intelligent Environment Interfaces

Some intelligent environments use unique, public interfaces to provide a specific service (e.g. Huang, Pulli & Rudolph, 2005; Vogel & Balakrishnan, 2004). But many more intelligent environments leverage the existing mobile computing resources that are prevalent in modern society (e.g. PDAs and mobile phones) to share information. These systems allow users to integrate the interaction with intelligent environments into their daily lives, and can provide a consistent interface for service discovery and usage. This section considers the required attributes of a user interface on these mobile devices. User interaction with an intelligent environment without the use of a public display (or a mobile device) is considered in section 6.5.2.

The interface used to interact with an intelligent environment will often determine how effective a particular environment is. Intelligent environments provide users with countless interaction opportunities that will mimic the interaction options available in the real world. Users within intelligent environments seek to dynamically manage the 'face' or persona they present to the world depending on their privacy preferences and changing interaction needs. Existing interface designs focus on this management of identity (Jendricke & Gerd tom Markotten, 2000) and on the personalisation of an environment's services to overcome the invisibility problem (Carmichael, Kay & Kummerfeld, 2005). Intelligent environments should adopt an open, non-proprietary interaction standard to encourage widespread adoption of the environment's architecture and to maintain a consistent interface for interaction with multiple environments. This lack of open standards has caused the death of previous mobile interaction systems (e.g. DoCoMo Friend Finder (Iachello et al., 2005)).

To manage a user's interaction with intelligent environments, the interface must identify any available environments and their services and present this information in a manner that is useful to the user. An environment could potentially be served by multiple intelligent environments, so there must be an effective manner of recognising these environments. User interaction is mostly likely to be at a service level, as we expect most interactions with an environment to be with its services and not between its users. Users should therefore be able to combine their preferred services from multiple environments into one interface, and have easy access to other users and the digital communities within an environment. This suggests that a similar method of dynamically advertising and accessing services should be used.

User interfaces should maintain consistent functionality independent of the intelligent environment the user is interacting with. This will prevent users from potentially having to learn a different interface for each environment they interact with. Such a system could use XML-like data fields to advertise environments and their services, and these could be readily personalised by including description information within the XML descriptors. This use of small
XML descriptors would also reduce the amount of data required to be transferred to the user's mobile device (i.e. only the data needs to be exchanged, not the entire interface program). This method would also allow users to choose their own interface, which they would be proficient in using, would easily allow for multiple languages to be supported and allow for easy personalisation of services and available environments.

Existing interaction interfaces that are familiar to users (e.g. web browsers) should be used for service delivery where possible. Where this is not possible, service aggregators could be used to create interfaces for specific services (or service classes). The iCrafter service framework uses an Interface Manager to combine services and hardware through the use of generic patterns that govern standard interaction commands and hardware capabilities (Ponnekanti et al., 2001). Development of a standard interaction library that could be used by any available services would be especially useful in combining ubiquitous computing services on the fly.

The provision of contextual data and conditional identities are an essential element in the personalisation of a user's interactions. Users must be able to represent their current interaction requirements and manage what data is passed on to an intelligent environment's service providers or to other users. Users' acceptance of an intelligent environment is, in many cases, directly related to the interface's ability to assist users in judging the potential benefits and privacy risks of an interaction. The development and testing of a specific user interface is beyond the scope of the dissertation. However, the required interaction capabilities are provided in the design of the intelligent environment architecture and associated infrastructure (in chapter six).

5.2.5 User Information Storage

The design of information storage becomes relevant when we consider the types of user interactions and services available within an intelligent environment. Users require secure, private storage space for personal information, interaction histories and contact information. Intelligent environments often seek to personalise a user's interaction with the environment to tailor interaction interfaces and service delivery, and to overcome the problem of service invisibility by promoting or hiding available services. This is accomplished by the environment having access to a user profile describing users' attributes, interaction histories and/or services and interaction preferences. How user information and interaction preferences are captured, and where they are stored and utilised, has a significant impact on the effect of the environment on the user's privacy.

Users will often want to allow a particular service to access some of their personal information. A service may require specific information to be accessed or personalised. This information could be stored within the intelligent environment, entered manually by the user or automatically by their device, or stored either in an external location, such as a personal webpage, or on the user's device. Each of these solutions presents challenges. Storing information on the device requires the mobile device to have more computing resources in terms of power and storage. Advances in
mobile devices computing and battery power allow more processing power for longer periods, but in turn, new multimedia services require more bandwidth.

Ubiquitous computing devices are normal devices embedded with some form of technology to provide new interaction mechanisms or interface options. Whilst mobile devices continue to grow in computational power, some of these devices are replaced by simpler devices embedded in users’ possessions (such as jewellery or clothing). The dissertation suggests that interaction with these devices will become more prevalent in the future, and it is prudent to allow for more basic interaction devices to be used in the developed architecture. This adds additional challenges when considering the encryption and interaction capabilities of these simpler devices.

The alternative of using a mobile device for personal information and pseudonym storage is the use of third-party storage located somewhere outside of the intelligent environment. If we assume that, unless there are mitigating security concerns, all intelligent environments are attached to the Internet, then this would be at least as effective as using a mobile device. This information storage would always be available, accessible across the Internet, free of battery or wireless connectivity problems. This centralised storage of a user’s personal information would provide a convenient method of providing access to the user, like an interactive business card, remove the burden of information storage from the user’s mobile device and prevent data loss in the case of losing the device. The interface device could provide an account to the intelligent environment and the interaction could then be personalised to any available mobile or public interfaces.

Further research that the author is involved in recommends the use of an external repository to store personalisation preferences for heavily customised devices (i.e. mobile phones) (Häkkilä & Chatfield, 2006). A user’s interaction preferences could be stored on a central server, and an electronic link to those preferences could be provided to the environment when the user logs on. This could be used to support interactions with very simple devices or to link to the user's personal preferences for using public interfaces. However, this interaction method would not provide the user with the same privacy protections afforded by the use of devices capable of managing the user’s personae and providing encryption for information exchanges.

The dissertation’s investigation into user perceptions of information sharing suggests that users normally avoid using security measures on their own device, instead preferring to rely on social customs to protect their privacy. This does not mean that there is limited value in securing users’ information on their personal device, but it does suggest that technologies related to security measures would be more profitably focused on the securing of users’ information within an intelligent environment and whilst it is in transit. The functionality required to interact with the dissertation’s infrastructure would be available in any modern smart phone or PDA. Security of individual devices should therefore be left to their owner’s discretion, with only a user’s interaction software needing to be secured (e.g. with a password) to prevent anyone from picking up a lost device and posing as its owner.
5.2.5.1 Securing Interaction Information

Storage of information within intelligent environments must acknowledge the conflicting desires of the data owners (the users) and that of the data collectors (the intelligent environments). Users want to limit the information provided to the environment when it is required, and to act anonymously and provide little to no information when it is not required. Intelligent environment designers require information on general usage of the environment, and access to users’ information, to allow personalised, and therefore more valuable, services to the user. An effective, fair intelligent environment must strike a balance between these contradictory goals to allow a useful intelligent environment to be developed whilst still being attractive to users.

There are three types of information stored within an intelligent environment: users’ personal details, their own interaction histories, and summaries of all interactions carried out with the environment and its services. The storage location and access rights to this information have a dramatic effect on a user’s privacy and acceptance. This information is described in Table 14. Each level of storage is secured cryptographically by the information owner using trusted computing components. This is an example of multilateral security.

<table>
<thead>
<tr>
<th>User’s Personal Details (secured by the user)</th>
<th>Information describing users’ attributes, interaction preferences, their mobile computing devices and any other personal information or data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User’s Interaction Details (secured by the user and the IE)</td>
<td>Interaction histories describing individual interactions with an intelligent environment and its services, including any identifying user information.</td>
</tr>
<tr>
<td>IE Interaction Summaries (secured by IE)</td>
<td>Summaries of all interactions within an intelligent environment. Information collected by the environment during an interaction or the delivery of a service is added to these interaction summaries without identifying user information at the time of the interaction.</td>
</tr>
</tbody>
</table>

Table 14: Information Storage within an Intelligent Environment

The user’s personal details are secured by the user’s public key on either the user’s mobile device or within the intelligent environment. This information can only be accessed by the user when interacting with the environment, and cannot be accessed by the intelligent environment for other purposes. Storing information within the intelligent environment allows the environment to confirm the information when it is initially provided, and therefore provides a more streamlined interaction process than if the user had to provide access to their identity broker each time they wished to interact with a service. Securing information on a potentially untrustworthy third party’s hardware calls for the use of trusted computing components to secure the information in a way that cannot be accessed by the third party.

The second category describes information generated by both the intelligent environment and the user. This information must be available to both parties, but there are limitations to what the parties can do with this information. Users are prevented from exporting the information en masse, to prevent potential multiple users from colluding a service’s outputs in an attempt to understand a service’s method and to predict likely outputs (this is only likely
in extreme cases). Similarly, intelligent environments are prevented from extracting individual interaction records (linkable to a pseudo-anonymous user ID) and using this information in other areas (and violating natural borders of privacy). This practice could easily lead to methods of identifying users through mining service usage and recognising interaction preferences or techniques in common between users.

The final category holds summaries of all interactions within the intelligent environment (or for a particular service), and this information is secured (and only accessible) by the intelligent environment. This security allows information to be built up over time, thus improving the depth of personalisation that can occur, without breaching the users’ privacy by allowing their information to be accessed without their permission. This use of anonymised data is recognised as a manner of allowing the use of valuable interaction information without breaching the user’s privacy.

Storing information on the intelligent environment leaves the users open to inference attacks, as potentially multiple services could be provided by the same operator. It is therefore important that users understand the threats posed by multi-attributive matching and data surveillance (Clarke, 1994). To reinforce the user’s ownership of data (identified in Table 14) users must have an easy to use method of removing their information from the system. This might be via a direct ‘delete user records’ link, which would delete all user records and leave only anonymous interaction data. If provided the user’s mobile device could easily delete all of the user’s interaction records (across a number of services) when so directed. The storage of information within an intelligent environment is considered in section 5.3.3.

5.2.6 Design Conclusions

This section describes the necessary characteristics of a ubiquitous computing infrastructure that can provide ubiquitous computing support through a network of individual intelligent environments. This infrastructure could therefore be used to provide ubiquitous computing services throughout users’ everyday lives. While the role that these environments will take is unclear at this stage, their potential is enormous. The ubiquitous computing infrastructure could provide new interaction venues to promote interaction between members of communities.

Existing intelligent environments focus on methods of interacting with the environment, specific services that adapt to contextual conditions and the storage and representation of a user’s personal information. This overlooks additional benefits that could be realised by providing community interaction spaces using ubiquitous computing technologies. These technologies overcome key limitations in more traditional digital communities that do not provide the same sense of presence or localisation (i.e. the feeling of being connected to the local community), or have the same accessibility that would be achieved using this ubiquitous computing infrastructure. These digital communities should begin to address the lack of community connectedness that many of our communities have lost along with our ‘third places’.
The other important consideration for our infrastructure’s design is what services users will require, and what support structures will the infrastructure require. Intelligent environments require two basic types of services: environmental services provided by the intelligent environment and global services that the user interacts with through the intelligent environment. These services require the existence of external entities to allow users to prove their identity without requiring lengthy pre-interaction configurations when a user enters an environment for the first time. The infrastructure must also allow anonymous, secure interaction with external services. This increases the value of the intelligent environment to users and allows users to determine for themselves what information they wish to expose.

The identity management entities required within an intelligent environment depend on the goals of the user’s interaction. Third party routers for user-to-user information requests improve the user’s anonymity and prevent intelligent environments from gathering information about the user without their permission. Identity Brokers provide trustworthy, centralised confirmation of the user’s identity or personal information. The use of signed templates allows users to interact anonymously (or pseudo-anonymously) with service providers in the same way that we interact with merchants in the real world.

The presented solution must provide secure methods of interacting with the environment and its services, and allow the user control over what information or persona they share with the environment based upon their interaction needs. Any interaction interface must manage the user’s previous interactions with the intelligent environment or service, and must provide users with the information they require to determine the effect of an information exchange on their privacy. The interaction interface should also be independent of the environment the user is interacting with, and should build lists of available intelligent environments and services dynamically based upon those advertising their services in the area. Information stored within the intelligent environment is secured by the user and the intelligent environment in a way that will prevent the user’s information from flowing to other environments, thus avoiding accidentally breaching the user’s privacy by crossing natural borders of privacy.

### 5.3 Intelligent Environment Design

Intelligent environments have the potential to revolutionise the manner in which we obtain commercial services and interact with our daily environments. Intelligent environments generally consist of a mobile computing interface interacting with an invisible services infrastructure that is contextually aware of its environment. The context-awareness provides the ability to personalise services based upon the user’s (observed or specified) preferences and the current state of the environment (e.g. number of occupants, time of day etc.). This research examines how these goals can be delivered without impacting on the user’s privacy, considers the required security for the user’s handheld device and their environment, and considers
a holistic approach to the development of multiple intelligent environments across all of our everyday spaces.

Intelligent environments have finally reached the stage where they are being deployed in the real world in pilot programs and demonstrator environments (refer to section 2.3.1). These environments are being used to test wireless networks, investigate user behaviour and privacy concerns and to reflect on their place within our world. But it is worth noting that, at this early stage of development, it is impossible to predict which intelligent environment services will become widely adopted. It is therefore more important to determine how a wide range of services can be delivered.

Generally speaking, intelligent environments’ services can be classified into two main areas: Environmental Services and Global Services. Environmental services provide users with local information (e.g. bus timetables, local events, directions etc.) and interaction opportunities (e.g. purchasing a movie ticket, opening a secured door etc.). Global services provide access to user-centric services (via connection with the Internet) that are not related to the local environment (e.g. accessing a news or reference website, connecting to communication tools (MSN, VoIP etc.) or searching the Internet). Both of these categories include ‘Community Services’ that promote engagement with the community, or interaction between members of the community within the environment (e.g. digital community message boards, chat rooms or other community engagement services).

Environmental services provide the user with local information and access to environmentally-based services. Examples of these services include providing access to secure areas (by opening security doors) or receiving information on the latest sales in a shopping centre. These services often require confirmation of part, or all, of a user’s identity to control access to a service. Users may often appreciate the ability to personalise the service interface and interaction based upon their preferences and past interactions, and the intelligent environment therefore needs to be able to create, improve and store these preferences. These interactions all need to be private and secure, preventing the unauthorised collection of personal information or interaction histories that endangers user privacy within these types of environments.

Global services are environment independent services that allow users to manage their interaction within the digital world. These are services that allow users to interact with the Internet, and through it make use of services previously available via a more traditional computing infrastructure. Examples of these services would include accessing Internet-based communication tools (e.g. instant messenger (IM), email, VoIP etc.) and interacting with centralised information websites and systems (e.g. accessing Google, news websites or use of RSS or Atom web feeds). To allow anonymous interactions with these external entities, users need a secure, private method of accessing the Internet through an intelligent environment. Any intelligent environment architecture that seeks to provide a holistic approach to using ubiquitous computing to support users’ lives must allow anonymous secure interactions and provide users with privacy when accessing environmental services.
Chapter Five: Privacy Requirements for Ubiquitous Computing Systems

Community services cover all services designed to provide, or improve existing, interaction between members of the community. These services include computer-mediated communication (CMC) environments, encompassing chatrooms, multi-user environments or bulletin board systems that allow users to interact with other members of the community. These systems have shown potential in improving the ‘social connectedness’ within a community, addressing the increasing disconnectedness of modern suburban cities (Oldenburg, 1999). These services should allow anonymous interaction to promote the system’s use, and should allow access to localised community interaction services from external locations to promote community access and improve the effectiveness of the service. Community services could be either local or global, depending upon where they are hosted, but would normally be served locally in the community they are based in.

This understanding of the potential services provided by an intelligent environment provides us with some design constraints for the architecture. Intelligent environments must provide a secure, anonymous infrastructure for users to interact with the local environment, and with local and global services. The need for third-party identity confirmation also suggests that access to the Internet is required. Users may need to prove their identity through the provision of an identity account, registered with a third-party identity broker. Properly designed, these structures should allow users to maintain control of their identity and to manage the risks to their privacy during any interaction with an intelligent environment.

Intelligent environments have the potential to cover every aspect of our daily lives, so we suggest considering the formation of a pervasive infrastructure made up of multiple, potentially overlapping intelligent environments. This infrastructure would allow users to be connected to physical places via their intelligent environment across the Internet (or from other intelligent environments). This access would also allow users to interact with their existing Internet productivity and communication tools, greatly enhancing an intelligent environment’s value. By envisaging a global infrastructure, we can consider what types of structures we require (such as the external identity manager) and consider how the use of each of these structures influences a user’s ability to interact with multiple intelligent environments without risks to their privacy or security.

The dissertation’s intelligent environment architecture (described in chapter six) will form the basis for our ubiquitous computing infrastructure, and thus must adhere to the design goals within chapter five. Intelligent environments will be as diverse as the services they provide and the environments which they inhabit. Our architecture must allow this diversity to be expressed whilst maintaining a secure and private generic communication infrastructure. This section examines the social and technical requirements of the ubiquitous computing infrastructure and expresses these requirements as design goals for the intelligent environment architecture described in chapter six.
5.3.1 Information Flow

Users’ fears about intelligent environments relate to their ability to collect and share vast amounts of personal information without their knowledge or consent. To overcome these fears we must provide a transparent method of anonymously interacting with intelligent environments, and add to this a method of visualising information exchanged with an environment. This provides users with the ability to understand what information about themselves is provided to an environment (and why), and to determine for themselves whether the benefits of this exchange are worth the cost to their privacy. This section is focused more on the control of users’ information within an intelligent environment than on the development of a particular architecture, but design recommendations for our intelligent environment architecture are highlighted.

An intelligent environment architecture must determine what mix of multilevel and multilateral security is required to secure environmental transactions and users’ personal information. Multilevel security involves securing data based upon the escalating likelihood of it infringing a user’s privacy (e.g. classifying some personal information public, secret or top secret). Multilateral security involves the securing of information based upon the likelihood of the type of information (e.g. all payment information) endangering a user’s privacy. The dissertation’s architecture will predominantly adopt multilevel security by securing access to user data that can have a negative impact on their privacy (such as identity information or location information). It is likely that a mix of these approaches will ultimately be adopted, with information being initially restricted by its type, and further controlled within a system (e.g. controlling access information within an environment’s service).

Intelligent environments can be implemented over a wide area to support a specific user group, service type or physical location. An environment might provide council services and directions for an entire neighbourhood or city, make available support services to a particular religious or special interest group, or provide advertising and shopping assistance to shoppers in a suburban shopping centre. This means that users in any given environment could easily have access to dozens of intelligent environments, each with a variety of services. This, combined with the design goals of keeping these services unobtrusive (or invisible) within their environment, means that users could easily lose the ability to readily identify and understand the available services and their impact on users’ privacy. Therefore, the first aspect of managing the flow of information is the identification of useful services and intelligent environments, and the personalisation of what information is displayed on their mobile device.

Intelligent environments require an effective personalisation mechanism that does not require users to provide interaction or service preference information to the intelligent environments upon entering their physical environment. A standard method of exchanging information quickly without undue strain on the environment’s wireless network is also required, and any personalisation of an interaction interface should therefore occur on the user’s mobile device. Modern messaging systems based upon Universal Plug and Play (UPnP) or
multicast DNS (mDNS) messaging provide lightweight, flexible service discovery. Of these protocols, mDNS is more useful as it has extensive Service Discovery mechanisms and it can more readily handle any new application-layer protocols that may be required in an intelligent environment architecture (Cheshire & Steinberg, 2006).

The user studies in the previous chapter highlight the need for effective feedback on information exchanges within an intelligent environment. The identities and information collection policies of intelligent environments must be provided to users before interaction takes place. Other feedback on an information exchange must include previous exchanges with this party, identification of all information shared (including environmental sensor’s collection activities) and its planned usage, and the expected outcomes or service goals. Users will consider this feedback along with their perceptions of exchanging information within the current social and market environments, the exchanged information’s sensitivity and the risks or benefits of providing the information or accessing the service.

Systems that provide feedback on the trustworthiness or reputation of other entities, services or users further assist the user in determining the impact of an information exchange on their privacy. Trust and reputation systems should be integrated into the dissertation’s architecture to allow this feedback to be gathered from independent sources outside the intelligent environment. This information won’t always be available, especially considering our requirements of allowing users to anonymously interact with the environment. Therefore, these systems will be considered as an external service that users can access via the intelligent environment’s wireless network.

The ability to effectively evaluate the impact of sharing information within an intelligent environment is essential for users to make informed decisions as to the impact it will have on their privacy. This in turn allows the users to accurately reflect their interaction (and identity sharing) requirements. The dissertation’s architecture must therefore provide the user with as much useful information about the environment as possible. Users’ understanding of the risks to their privacy of an information exchange (or service utilisation) will allow them to determine what information or persona they would like to share with the environment or service.

User desires for privacy will be coded into their privacy preferences (on their mobile device) and are expressed when users initiate or approve an information exchange. To further personalise their interaction preferences, users should also be able to describe their current motivational or interaction requirements to their mobile device. The need for adequate feedback and effective user control over information sharing with an environment must be tempered by the need to maintain an easy-to-use interface that does not overwhelm the user with information. This must be informed by the work on the invisibility of ubiquitous computing information and services described in section 2.3.5.

The use of sensors to gather information on users without their knowledge is central to users’ privacy concerns about information collection in intelligent
environments. The use of sensors must be limited to gathering information about the environment for service delivery. Users’ personalisation information should only be provided by the user, to ensure they have control of its distribution. In most cases this type of invasive monitoring will greatly reduce the value of an intelligent environment to its users (and thus will have an impact on its service usage). When it is required, monitoring users and their interactions should be limited to unique, clearly defined areas where this type of invasive security is justifiable. The use of contextual information should clearly be expressed to users before they initiate any interaction with the environment. This enables users to opt out of interaction, potentially by limiting access to environments with certain types of information collection activities through the privacy preferences they set on their mobile device.

Security is important within intelligent environments, as they are often comprised of untrustworthy components that may be physically accessible to users within the environment. Information flows between all elements of an intelligent environment must be secured where possible, and information that cannot reasonably be secured (for example because the sensor doesn’t have the computational power) should not contain identifiable user information. Intelligent environments should therefore seek to have the information that is shared between entities capable of providing effective security (i.e. computationally capable of using encryption). A Kerberos server is used to ensure the confidentiality and integrity of all communications within the environment. To avoid the collection of users’ mobile device’s MAC addresses (or their globally unique ID), and to prevent third parties linking users’ interaction sessions, the users’ mobile devices must use randomised MAC addresses during their connection.

The Gaia OS (described in section 2.3.2.3) demonstrates an effective method of securing the destination and contents of a particular packet of information, regardless of the network the message must pass through. This method of securely routing information across a network is integrated into our architecture to provide users with confidence that any information exchanged through the intelligent environment will not be collected. Users could use this obfuscation technique to route service requests to external services via their identity manager. Any third party attempting to collect information on the user’s service or interaction habits by examining these requests would therefore only be able to determine the IP address of the user’s User Manager. The User Manager would likely have enough customers that determining the user’s identity by this information alone would be infeasible.

5.3.2 Identity Management

Identity management is about more than authenticating identity assertions made by the user. It is also about the desire of users to accurately control what personal information is shared during a particular information exchange. This might incorporate the need for anonymous or pseudonymous interaction with an environment and its services. This ubiquitous computing infrastructure requires identity providers that are globally accessible to allow services to authenticate a user assertion of identity. These centralised identity
providers will build up trust with service providers and users over time, but they must maintain a user’s privacy.

The primary identity provider in our architecture is the Identity Broker. An identity broker provides a third party that allows users and intelligent environments alike the ability to authenticate assertions of identity. Identity brokers will initially leverage real world relationships or reputations to generate some trust in their identity authentication service, but ultimately the trust placed in them will be determined by their handling of their clients’ identities and publicity of privacy breaches. Service providers can gain more confidence in an assertion by authenticating the user’s assertions with more than one identity provider.

These entities must support the use of a multiple personae and allow users to confirm only the parts of their identity, which, for example, would allow the verification of the user’s age or residence without the need to provide their name. This system will require the user to set up an identity account with the broker before use in an intelligent environment, but one identity broker can be used in multiple environments. Any use of an identity broker must be secure in order to allow the exchange of information without fear that a user’s information is being intercepted by a third party.

Identity Brokers require the intelligent environment to have access to the Internet over which to make the identity authentication requests. This requirement provides many opportunities to integrate globally accessible services into the fabric of the ubiquitous computing infrastructure. Intelligent environments, however, will not always have this access, and there may be times where the users may want to protect their primary identity by not using centralised identity brokerage services. Intelligent environments must, therefore, have local methods of confirming a user’s identity (or pseudonym). This can be accomplished by the intelligent environment maintaining user accounts for users to log into, or through the use of digitally signed templates that the intelligent environment can trust.

Intelligent environment based service accounts could be used to develop users’ interaction preferences (through the service adapting to users’ preferences over repeated use). They could also be used to leverage an existing relationship with the environment’s developer. For example, an office intelligent environment is likely to already know its users, and indeed may need to differentiate them to provide group awareness or productivity services. Whilst privacy is less of an issue in group awareness environments (users sign up to these systems to have their location information shared with other users), users can still interact with the former without concern if the information collected about the user is within their privacy preferences.

Control over which account or pseudonym the user utilises can also have a big impact on privacy, especially when the user’s information is provided voluntarily and not sensed directly by the environments. The interface used to interact with the environment must allow the user to visualise and control what information (or persona) is currently applied to a service interaction. The ability of the user to switch between pseudonyms or personae at will is
vital for maintaining the user’s privacy. For an example refer to User Selected Pseudonyms in section 6.4.3.

Digitally signed templates that have been signed by a (potentially) trusted third party are simple subsets of the user’s personal information. Users are unable to change a signed template, which allows the receiving entity to assign a degree of confidence to the provided information based upon the issuing third party (e.g. a university, community organisation or bank). A template could, for example, contain information on the user’s university enrolment status to gain access to university services without needing to provide their name or other contact information. As noted, templates are only as valuable as the trust placed in them by the receiving service or intelligent environment, and therefore are likely to be more relevant in their local area or home country. The use of these templates is evaluated in section 6.4.3.

Without the reusable pseudo-anonymous identities provided by the digitally signed templates, users would only have two options when interacting with intelligent environments: interact anonymously, which might be rejected for certain services, or interact with a subset of the user’s real identity. This middle-ground identity broker allows anonymous interaction with services whilst providing the service provider with some confidence that the user should have access to the service.

The method of communication between parties within an intelligent environment influences what security layers can be used, and ultimately how much trust users will have in the system. Collection of information on the path information takes to reach a user could potentially be as important as the encryption algorithm used. Any communication within the intelligent environment must be encrypted, not traceable to the user, not subject to data mining attacks to determine user information and not able to be linked to previous user interactions.

The dissertation’s architecture must use an Identity Manager so that users do not connect directly with the user’s personal domain. However, instead of giving the user's identity manager's location directly to the third party, the user could make use of blind relays to disguise the ultimate destination. The Gaia OS uses blind relays called ‘Mist Routers’ to disguise the ultimate destination of an information packet (Campbell et al., 2002). The privacy and security aware architecture could use similar routers to ensure that the information is not sent to a traceable location. A Kerberos server provides communication confidentiality and integrity by managing the key exchanges for all communications within and with an intelligent environment.

The use of identity management structures, such as the identity broker, has the potential to be abused. Users may decide to set up multiple user accounts to manage exposure to an identity while acting dishonestly, similar to criminals maintaining many different aliases. This could reduce users’ trust in providing identity information and ultimately put the use of identity brokers at risk. The problem could potentially be even greater when using trust-based approaches to user identification (Hitchens, Kay & Kummerfeld, 2004). The
use of plutocratic access control (see section 2.5.2.2) could make this gaming of the identity brokers infeasible.

A similar suggestion to prevent the misuse of identity accounts would be for users to provide a payment upon the creation of the identity account. This guarantee would be lost in the event of a breach of user conduct. Users would not ultimately have to pay unless they did something wrong. This would require a means to report malicious activities with an identity broker and some sort of industry code regarding the use of payment guarantees. This type of feedback could be entered into a trust or reputation system, whose use is described in section 6.5.4.

5.3.3 Information Storage

The use of global identity management structures does not exclude any type of information storage within intelligent environments. Intelligent environments must define how information is collected and where it is stored, and consider what interaction methods would allow the user the most control of their information whilst maintaining their privacy. User information used within intelligent environments can be stored in three places, each of which has different impacts on privacy and security. These include storage on the user’s mobile device, storage within the intelligent environment, and online storage called remotely via the environment’s Internet access.

Mobile computing devices have only recently reached the stage where large data storage is possible, but its use may not be warranted. The Personal Server (see section 2.3.2.5) reverses the traditional thin-client paradigm of mobile interaction with service providers with the user’s information already residing on the user’s device. This reduces the information that must be exchanged through wireless communication and allows the users more control over their data. This section examines the advantages and disadvantages of storing the user’s information on their mobile device (in some ways replicating the Personal Server approach), with the intelligent environment, or within a user-controlled third party accessible via the Internet (e.g. a Personal Domain).

The three types of information required within the intelligent environment to allow users to effectively interact with the intelligent environment and its services are described in Table 15. Multimedia and application data refers to user-owned information that users want to share or provide to an application (e.g. a user’s media files or service database). This information is owned by the user, and any exchange of it must be within their privacy preferences. User information and identity accounts refer to basic user information and accounts that the user holds to confirm their identity. The size of this information is generally relatively small, and may be limited to an encrypted identity account number or user-selected alias.

Interaction histories and user accounts refer to the user’s service interaction histories and the user’s method of identifying themselves to the server. This information would generally be comprised of the user’s personal information (e.g. information entered to obtain the service or personalisation of the
service), the user’s interaction preferences and histories, and anonymous summaries of service interactions for system development and maintenance. The storage of interaction information is described in section 5.2.5.

<table>
<thead>
<tr>
<th>User Information Storage Location</th>
<th>Information Specific Issues</th>
<th>Privacy Concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device</td>
<td>Multimedia, Applications, etc.</td>
<td>Quicker access to and communication of information; Offline access; Potential data storage limitations.</td>
</tr>
<tr>
<td></td>
<td>User Information, Identity Accounts, etc.</td>
<td>Effective user control over identity information exchanges.</td>
</tr>
<tr>
<td></td>
<td>Interaction Histories, User Accounts, etc.</td>
<td>Ability to personalise common services in new environments (e.g. load preferences etc.); Potentially large amounts of info. to exchange (slower service interaction); Easier (offline) access to interaction histories.</td>
</tr>
<tr>
<td>Intelligent Environment</td>
<td>Privacy concerns when providing information to untrustworthy environments; Information must be as mobile as the user.</td>
<td>Storage of this information would breach privacy design conditions of reducing availability of info. to data users; Requires identity negotiation (account setup etc.) with the environment prior to use.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interaction histories essential for effective service delivery; Requires encryption or access control to prevent reuse of this information for other purposes.</td>
</tr>
<tr>
<td>External Domain</td>
<td>Large information sizes require lots of bandwidth for external use; Allows for simpler interaction devices (i.e. reduced storage, transfer bandwidth and encryption capabilities).</td>
<td>Provides external identity authentication / response to enquirers; Reduces cognitive load on user and user’s mobile device; Automated exchange replaces user’s intervention in identity exchanges.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure external storage allows personalisation of common service in new environments (e.g. load preferences etc.); Potentially large amounts of info. to exchange (slower service interaction); Easier (offline) access to interaction histories.</td>
</tr>
</tbody>
</table>

**Table 15: Information Storage in Intelligent Environments**

Table 15 highlights the privacy concerns that arise when storing personal information within the intelligent environment. This is also not practical for interaction with multiple intelligent environments, as the user’s information is then stored multiple times in different locations, which is time-consuming and can lead to data inaccuracies. Intelligent environment storage of interaction histories or limited user account information is useful, however, if this information is provided in accordance with the user’s privacy preferences, and if a manner to secure this information can be found. Section 5.2.5.1 discusses the use of trusted computing encryption to secure interaction information in a manner that benefits both users and intelligent environments.

Owing to their privacy concerns, users are much more likely to want complete control of their information, so we must consider the case for using mobile device storage (e.g. Personal Server) versus the case for using a secure, externally accessible storage area (e.g. Personal Domain). Table 15 compares these two storage choices. Both mobile devices and external domains allow
easier access to the user’s information, as they both can be accessed by the user anywhere. They also both provide users with active control over their information, something that is essential for user privacy. This, however, comes with a communication overhead as information must be transmitted (when required) to the environment via the Internet or wireless networks.

Personal domains can securely store information outside of the physical environment and communicate securely with an intelligent environment using encryption. Unlike handheld devices, personal domains can easily scale up processing power (for greater encryption) and use mains power (and thus are not limited by battery power). Their use could also lead to the use of simpler (and cheaper) mobile devices within intelligent environments, as they are increasingly used as a reference beacon that connects the intelligent environments to the user’s personal domain. This might lead to future interaction devices becoming smaller and smaller until they are embedded in clothing, jewellery or potentially replaced by biometric sensing of users. (The use of biometrics is fraught with potential privacy concerns, and is discussed as a future research direction in section 8.3.5).

The use of personal domains does have some drawbacks. As there is no user intervention, all information responses are automatically made according to the user’s privacy preferences. The user study in section 4.2.2 demonstrated that users have shown a strong preference for being able to manually confirm information exchanges. Exchanges that provide information to an intelligent environment should, where possible, allow users to confirm or reject an exchange.

Mobile devices with input and display capabilities are useful for eliminating the need for public interfaces (and the privacy concerns that come with their use). As mobile penetration rates in developed (and increasingly developing) countries reach saturation, there is also widespread access to these types of devices. These findings suggest that both personal interaction devices and personal domains have their place for interacting with an intelligent environment, and they will be integrated into our architecture in chapter six.

5.3.4 Design Conclusions

The design of an effective intelligent environment largely rests on the user’s perceptions of the privacy offered by the architecture. These sections have considered how to give users the ability to understand and control the flow of information within an intelligent environment; they have examined the identity management structures that are required to recreate the interaction opportunities and privacy protections we enjoy in the real world; and they have described the storage of information that occurs within the greater environment. These requirements are integrated into our final architecture in chapter six.

5.4 Summary and Conclusions

This chapter describes desirable characteristics of an intelligent environment architecture that forms the basis for a wide-scale ubiquitous computing
infrastructure. Specifically, this chapter examined: the ability of ubiquitous computing environments to act as digital third places in order to support community connectedness and social interaction; the impacts of the information flow within the environment on users’ privacy, and how information can be stored to prevent privacy breaches; and the required identity management infrastructure required to provide users with the interaction experience they require.

This chapter provides a set of characteristics with which to evaluate the interaction provided by existing intelligent environments. The user studies in chapter four in particular provide interaction guidance on the casual (anonymous and pseudo-anonymous) interaction capabilities that users want with intelligent environments. These interaction and identity requirements provide a set of design principles against which all intelligent environments can be judged. These design principles are incorporated into the initial architecture described in section 4.4, and they form the basis for the final architecture’s design described in chapter six.
Chapter Six: A Solution for Privacy in Ubiquitous Computing

6.1 Introduction
This chapter describes the intelligent environment architecture developed to provide users with a ubiquitous computing infrastructure that securely and privately provides ubiquitous computing services. This chapter describes the developed architecture and its functional requirements, and provides a sample implementation that demonstrates the relevant communication infrastructure. The architecture is then evaluated via user field tests, and solutions for further improving user privacy are discussed.

6.2 SPACE Architecture
The developed intelligent environment architecture was named the Secure Privacy Aware Communication Environment (SPACE) architecture, highlighting its role in providing a secure interaction environment for communication and service delivery using ubiquitous computing technologies. This architecture was developed through the evaluation of the current privacy, security and intelligent environments architecture research (chapter two), user studies investigating users’ reactions to these new environments (chapter four), and through our evaluation of the required role of these environments in forming a ubiquitous computing infrastructure across our everyday environments (chapter five). The SPACE architecture forms the basis for this ubiquitous computing infrastructure, enabling the deployment of intelligent environments across our everyday lives.

The SPACE architecture expands on the initial architecture described in section 4.4, particularly with regard to identity confirmation within intelligent environments. It describes the major components required to provide personalisable service delivery, private user interaction and the graduate identity management entities that provided varying levels of identity authentication. This architecture could form the basis for a scalable ubiquitous computing infrastructure that could support overlapping environments using the same identity and user support entities.

A high level representation of the SPACE architecture is detailed in Figure 12. This diagram shows the three identity authentication entities (Identity Broker, Information Service Provider and the Identity Manager/Personal Domain), the User Register and Service Providers and the user’s mobile device. The intelligent environment boundary shows that only the User Register and Service Provider are located within the intelligent environment, which provides an anonymous interaction space that allows users to enter and leave without requiring users to identify themselves or leave digital traces that could be used to recognise the user in future visits.
Figure 12: Secure Privacy Aware Communication Environment Architecture

The SPACE architecture has three main principles guiding its development. The first is the requirement for users to control their information wherever possible, including allowing users to visualise and manage the flow of their information within the environment (and between environments). This is done by improving user awareness of how information is being used, and through decreasing the amount of information that is made available to the intelligent environment. All intelligent environments and services must provide information on how they will use information provided by or sensed about a given user. This control of identity information exchanged with the environment leads to the second guiding principle.

Users must have control over how their identity is represented to the environment or its services. In doing so this architecture seeks to support the service interactions and identity control that users enjoy in the real world. To achieve this interaction, users ideally must be able to represent their identity in different (graduated) ways. These uses range from anonymous interactions with the environment and some services, to the verification of only part of their personal information using a trusted intermediary, to the ability to prove the user’s identity using a trusted broker. The SPACE architecture’s different identity management entities are described in sections 6.2.4, 6.2.6 and 6.2.7.

The final guiding design principle of the SPACE architecture is the need to consider how an intelligent environment would work as part of a larger, scalable infrastructure that could support multiple intelligent environments overlapping in the same physical environment. This principle urges the consideration of how identity management structures can be used between environments, how interactions with multiple environments could occur (potentially at the same time), and how users could integrate within this greater structure to access global services and maintain a consistent presence that manages these services whilst being resilient to poor wireless coverage and intermittent access by the user’s mobile device. This final requirement led to the development of the Personal Domain, a user-controlled persistent server that can manage users’ global services and provides an anonymous access point for communication with the user. The Personal Domain uses a blind routing system (the Identity Manager) to prevent the Personal Domain’s
address being used to identify the users. Figure 13 describes the SPACE architecture in more detail.

The user interacts with an intelligent environment using a mobile device. The device is used to identify intelligent environments (Flow A describes the initial negotiation of access to the environment), provide a service interaction interface (Flows G and I) and allow the user to interact with other users within an intelligent environment (Flows B & E). The mobile device is also responsible for managing the user’s interaction and identity sharing preferences (Flow H). The role that the user’s mobile device plays in this environment is discussed in more detail in section 6.2.1.

The User Register is responsible for the provision of information about, and the management of users within, an intelligent environment. As such, the main task of the User Register is maintaining an anonymous list of users connected to the environment, and providing information beacons that describe the intelligent environment, its owners, purpose and any privacy conditions associated with its use. Information Flow A describes the environment and gives a link to enable the user to find out more information. Upon connecting to the environment (Flow B), users can provide personal information (i.e. a description or alias) and potentially an identity management ID that could be used by another user to contact the user’s Personal Domain (Flow C). The User Register is described in more detail in section 6.2.2.

Each service provider within the current intelligent environment uses a beacon (Flow G) to advertise the service’s existence. The beacon describes the service, any privacy and information usage policies and gives the user’s mobile device a reference to access the service. The user’s mobile device connects to the service’s location (Flow I) and provides an interaction interface for the service. If required the service provider’s authorisation entity
is responsible for verifying the user’s right to access a service, potentially using either an Identity Broker (Flow J) or using a secured information template (Flow F). The service provider is described in detail in section 6.2.5.

As part of the graduated identity management approach utilised by the SPACE architecture, three different identity management structures interact with this intelligent environment. The Information Service Provider (see section 6.2.6) allows users to interact with an intelligent environment using a secure, digitally signed persona that the intelligent environment can use to verify subsections of the user’s personal information for service interaction. Identity Brokers (see section 6.2.7) are more traditional identity management entities (such as Banks or Government agencies) that can verify part or all of a user’s identity. The Personal Domains (see sections 6.2.4) are persistent online storage systems that allow users to manage global services and provide information about themselves in a way that does not immediately endanger their privacy whilst within an intelligent environment.

6.2.1 User Mobile Device

The SPACE architecture requires the use of a mobile computing device to access the intelligent environment and interact with its users and services. This device contains the Persona Manager, to control the information users share with the environment, the User Manager, which maintains a list of all users within the environment, and the Service Manager, which provides access to all available intelligent environment services. The user’s mobile device also maintains the GUI used for interfacing with these information interfaces. The user’s mobile device is described as part of the architecture in Figure 13.

The type of device used to interface with the intelligent environment could vary considerably between users. Mobile phones and Personal Data Assistants (PDAs) are the most likely devices to be used given their current pervasiveness, but other input and display devices would also work. The interaction device and infrastructure must support multiple concurrent processes, either using the same or different identifiers (or interaction personae etc.), allowing the user to connect to the intelligent environment as many times as the user requires. These concurrent processes must also each use a different randomly generated MAC address to further protect the user’s privacy.

The User’s Mobile Device provides a single sign-on for each of their personae, allowing the user’s to authentication their access once and the use the device to select which identity (or personae) they wish to interact with. The SPACE architecture allows interaction with the user’s environment with limited information exchanges, consistent with the design goals (in section 5.3.3) of allowing the use of simpler and cheaper interaction devices (with presumably more limited computational capabilities). These simpler mobile devices would manage the interaction with the environment, while the user’s Personal Domain would store their personal information and communicate with the environment.
The interface used to interact with the intelligent environment would be developer specific, and could vary depending upon the user’s mobile device and operating system. The requirements for the interface are as follows:

- The interface must provide the user with an overview of available intelligent environments within their current area, including all information on the intelligent environment’s description beacon (see section 6.2.2.1).

- When connected to an intelligent environment, the interface must provide a list of all public user profiles that are currently logged on to the user register (see section 6.2.2), including any information on the users that has been made public (6.2.2.2).

- The interface must present the user with a list of services being advertised within the current environment, including the information provided by the Service Beacon (see section 6.2.5.1).

- The interface must provide the ability to review previous interactions with an entity (either an environment, service or another user) and provide appropriate feedback (see section 2.4.8 and 5.2.4) on these information exchanges.

The interface used to interact with the SPACE architecture will form a large part of how effectively a user can manage their information within intelligent environments. The feedback provided to the user allows them to make informed decisions on the impacts to their privacy of using a particular service or persona. The interface must be able to provide minimum amounts of information (or default personae) to the environment in line with the user’s privacy preferences. Overall users must have control over the interaction experience, either directly via the approval of a particular interaction or indirectly through the setting of user privacy preferences and current interaction goals.

### 6.2.1.1 Persona Manager

The Persona Manager is responsible for managing the personae used to interact with the intelligent environment that describes a subset of the user's personal information. These personae are used to share information with an environment, for public presentation, or with a service in order to either personalise the service interface (or its delivery) or to prove the right to use to a particular service (e.g. by providing evidence of identity). Each persona utilised by the user is configured via the interface on the user’s mobile device and is completely under the user’s control. This allows users to maintain control over their personal information, and provides an efficient method of sharing information when given a reason to do so.

Each persona stored on the user’s mobile device has a different subset of the user’s personal information for exchange with the intelligent environment under different circumstances. The persona shared with the intelligent environment at any given time is dependent upon the user’s privacy preferences and the user’s current interaction requirements. Maximum privacy is achieved by providing no persona or Identity Manager account to the intelligent environment. However, this anonymous interaction may not
provide the user with access to all the services within an intelligent environment.

Each persona is stored using an XML-like format to allow the easy exchange of user information. Existing user modelling languages could be used to create powerful and flexible user models that share a part or all of a user's personal information. The 'Personis' (Kay, Kummerfeld & Lauder, 2002) and UserML markup modelling languages, described in section 2.3.4, provide user information in a lightweight and flexible way that can be easily shared across multiple intelligent environments. Users would determine which persona to share with the environment depending on their information sharing goals and their perceived privacy risks of interacting with their current intelligent environment.

When a user enters an intelligent environment, their mobile device connects to the environment and provides their public profile to the User Register (refer to Information Flow A in Figure 13). This information includes any personal information they wish to share with the environment (e.g. name or alias, photo, contact details or interests) and their Identity Manager information (address, encrypted ID and public key). The identity manager (see section 6.2.3) provides an anonymous method for other users to enquire for more information about the user. This information is supplied directly by the user's Personal Domain (see section 6.2.4) without the information being made available to the intelligent environment. During connection the user must be able to specify that no identity information or persona be shared with the intelligent environment.

A user's persona manager has a number of (user configurable) interaction settings that describe their current interaction desires. These settings affect not only what persona is exchanged, but also how the mobile device interacts with intelligent environments. These interaction settings include:

- Passive: Normal service interaction. Only access service when explicitly asked for by user (this would be the default mode).

- Active: Actively use all information services that do not require identity authentication for interaction. All other services are accessed by explicit user instruction only. (This might include downloading news and local information from anonymous local and global services).

- Anonymous: Do not allow the provision of any identity validation or information to any services or environmental constructs. Warn user of any flagged intelligent environment surveillance.

- No Interaction: Setting used to ignore all local intelligent environment services and users. This setting would be used (as opposed to just turning off the user's mobile device) to still allow access to global services (those outside the current intelligent environment) and to other functions of the mobile device (phone, other applications).

The persona selected (either manually or automatically by the persona manager) for interaction with the service could be configured with information that assists in the personalisation of service delivery. Personalisation should,
where possible, occur on the user’s mobile device, but in some instances it would make sense to provide information to limit the download of information or an interaction interface to the user’s mobile device. The user has the option of selecting a preferred language for a persona, prompting the user’s mobile device to ignore interfaces in all other languages.

Where server-side personalisation is desirable, more sophisticated personae containing service personalisation information can be used. This personalisation information is provided to the Service Provider (see section 6.2.5.2) upon connection. The management of these personae will determine their risks to the user’s privacy. The more personal information that is on the persona, the greater the chance the service provider could either link the user to other interactions or potentially link the user to their real identity in other ways. Either outcome represents a huge risk to users’ privacy. These risks can be minimised by reducing the personal information used on the interaction persona and through using many different personae, each with different interaction information (see User Selected Pseudonyms in section 6.5.2).

The Persona Manager is also used to manage the secure digital templates that can be used to provide verifiable personae to an intelligent environment’s services. These templates can be used for pseudo-anonymous interaction with service providers whilst only providing a specific subset of the users’ personal information. This interaction tool provides access to restricted services without requiring users to identify themselves. These templates are obtained from the Information Service Provider (ISP) and normally leverage existing identity relationships with either the ISP or by providing an Identity Broker’s details with which the information can be verified. The method of obtaining these secure digital templates and their interaction with services is described in sections 6.2.6 and 6.2.5 respectively.

6.2.1.2 User Manager

The User Manager maintains a list of all users within the environment that have selected to make some of their personal information public. The User Manager provides a list of all users, including their public information, and allows the user to request more information from another user. These information requests might be used to confirm a user’s identity, allow a user to learn more about another user before approaching them or to exchange contact information. Information requests are forwarded securely through the intelligent environment to the user’s Identity Manager, and from there to their Personal Domain.

The User Manager connects to the User Register when the user moves into an intelligent environment. The User Register broadcasts information about the intelligent environment so that potential users have some information about the environment before they log on. This allows users to make a determination about the impact to their privacy of interacting with the intelligent environment. This information must be displayed for the user on their mobile device, and should be used by the user and their mobile device when deciding manually or automatically what information to share.
This broadcast includes the environment’s public key that is used for the initial connection with the environment. The intelligent environment and the user’s User Manager then exchange a session key to encrypt all traffic between the two. This exchange could occur using the environment’s local public key, but would be more secure using a centralised Kerberos system to provide time-stamped access tokens to the environment’s users. For more information about the User Register refer to section 6.2.2.

After the User Manager connects to the intelligent environment, the User Register returns a list of all users within the environment. This list contains the public information that the users have chosen to share about themselves. The User Manager interface can then be used to request more information about an individual user. This request is encrypted using the intelligent environment’s session key and passed to the User Register with the second user’s public key. This response is then forwarded to the second user’s Identity Manager where it is evaluated and forwarded further onto the user’s Personal Domain. Returned information is encrypted using the user’s public key and passed back to the User Manager either via the intelligent environment or directly via a real-time link. This may be required for VoIP connections (e.g. Skype), instant messenger (MSN, Yahoo, AOL etc.) or any other interactions requiring the two parties to communicate in real time. Depending upon the environment and architecture’s design, the exchange of encryption keys could be managed using a third party system, e.g. Kerberos.

6.2.1.3 Service Manager

The Service Manager provides the user with an interface to all the services available within an intelligent environment. It manages users’ interactions with a service by providing them with service information, previous interactions that the user has had with the service and links to any other information gathered about the service from third parties. This information allows the user to better assess their trust in the service, and in turn allows the user to better control what personae should be used and when. This interface displays all of the services that have been broadcasted in the local area by the Service Beacons.

Each Service Beacon describes the service, provides a local link to its interface and provides descriptive keywords that can be used to personalise the service. The Service Manager uses these keywords to personalise the interface, only showing services that are deemed relevant to the users (or those that match the user’s preferences). Further description of the Service Beacons, and the information provided to the Service Manager, can be found in section 6.2.5.1. This client-side personalisation allows effective personalisation of the available services without providing information to the intelligent environment, which has the potential to breach the user’s privacy.

The Service Manager manages a user’s interactions with particular services. The Service Manager interfaces with the Service Provider to build an interface that is used to obtain a service, and the interface automates the provision of the user’s identity information to the Service Provider. Intelligent environments’ services often need confirmation of identity before a particular
service can be accessed. The identity provided is selected from the Persona Manager, which displays all available user personae that can be used within the user’s current environment, and these identities are validated in three ways. Users can provide information on their identity themselves, they can provide a third party to allow external verification, or they can provide an information template that is digitally signed by a trusted third party verifying their information. The identity management system used with a service will depend on what it is accessing and the level of identity authentication required.

Users can provide their own details to a service in a number of instances. Some services would make use of user accounts to provide a repeatable experience for the user and to allow for personalisation of the service interface. Users could set up these accounts when first using the service, and would simply provide an account number (and possibly a password) in subsequent interactions. Whether or not the user’s identity would be necessary to create these accounts would depend upon the individual service. The utilisation of multiple accounts in a way to obscure or obfuscate a user’s interactions with a service is described as User Selected Pseudonyms in section 6.5.2.

Secondly, users could use an information template digitally signed by a trusted third party that asserts a subset of their personal information. When accessing a service, users would provide the service provider with a template describing the persona they wish to use, and the service provider would then make a trust determination based upon who signed the information. To improve the relevance of the trusted third party, this process would most likely be implemented on a small scale, using trusted entities familiar to the service provider or the environment. For example, a university might provide signed templates to students to allow them to prove they have the right to access a service without revealing personal information such as their name or student number. This trust-based identity management scheme was first described by (Hitchens, Kay & Kummerfeld, 2004), and its integration with the SPACE architecture is described in section 6.2.6.

Finally, we have adopted an approach that replicates more traditional identity management by using accounts with trusted third parties to authenticate user’s assertions of identity. This identity schema could be implemented using the existing Shibboleth, U-Prove or Liberty Alliance identity frameworks. This process is similar to traditional identity authentication that would be provided by an identity card or credit card issued by a government agency or banking institution. The physical cards provide proof of an account within the organisations that all parties can trust. In the same way that an account can be held within an online Identity Broker, this can be referenced by the service to confirm part or all of a user’s identity. The use of Identity Brokers for confirming identity is discussed further in section 6.2.7.

6.2.1.4 Privacy Threats and Analysis

The user’s mobile device is the least secure aspect of this intelligent environment. Users often lose their devices, fail to use basic security features
(e.g. keypad locks, etc.) and rely heavily on social norms (e.g. interaction behaviours) to secure the privacy of their mobile devices (see section 2.5.2.4). The protection provided by social customs may be more relevant when considering the use of text messages and more direct communication, as it is unlikely to provide sufficient security for devices that can in effect act as a proxy for the device’s owner. For example, a personal computer set up to represent a user could be used by a third party to access their email or restricted services, enter restricted areas or provide information to an environment in a way that violates their privacy preferences.

The security of such devices should be investigated when these systems are implemented on a mass scale. Potential added security could include the use of passwords with needy devices (i.e. the device requires the user to confirm their identity after a certain time or when the device is used in an unfamiliar manner); the use of biometrics to actively confirm the user’s identity when in use; or the use of biometrics to recognise the user and provide interaction based upon that identification. The privacy issues associated with the use of biometrics are numerous, but a complete discussion of this topic is outside the scope of this dissertation (see section 8.3.5). User training on the privacy implications of persona use would be of great benefit to users, particularly for service-heavy or wide-area environments, and for users from less technical backgrounds. Training should also examine the encryption, interaction and communication protocols that are used within the SPACE architecture to help ease the privacy fears of users when they initially encounter intelligent environments.

### 6.2.2 User Register

The User Register maintains a record of all users within the environment that have explicitly allowed their presence to be detected through the setting of their privacy preferences. The User Register provides connected users with lists of all other users within the environment, and users can use these lists to request more information from the user’s Identity Manager and Personal Domain. The information provided about a user to the wider environment is the information that user has specifically designated to be viewed by the public. The User Register provides a secure and anonymous method of connecting to the environment without subjecting the user to risks of their interactions being linked to previous visits in this or other environments.

The User Register is also responsible for broadcasting information about the intelligent environment to its potential users. This information, broadcast using multicast DNS (mDNS) messages (Cheshire & Steinberg, 2006), contains information about the environment’s owners, its purpose and potentially the services that can be obtained from it. This information is then used by the user to determine whether they should interact with the environment. The connection process is described in more detail in section 6.2.2.1. The interaction between the user’s mobile device and the User Register is described in Figure 13.

This structure could also allow users to connect to third parties outside of the intelligent environment, such as friends in different environments or the user’s
homepage. This is useful for allowing new forms of interactivity to emerge within these environments, and provides an incentive for users to use these environments. The exact nature of the third parties that can be connected will be dependent on the available resources (e.g. bandwidth) provided by the intelligent environment. This architecture provides a mechanism for these connections that do not make the user susceptible to privacy attacks or expose their information through unsecured communication channels.

Intelligent environments that use sensors to gather environmental information must warn users of this before they connect. This notification should be contained within the User Register’s Beacon (see Figure 14), and this could potentially trigger a warning if the user’s privacy preferences are exceeded. For example, Belinda (from our previous scenario in section 5.2.1.4) might prefer to receive a warning before she enters an environment that uses video surveillance, which allows her to either adjust her behaviour accordingly or leave the area under surveillance. As the beacon is used as an initial source of privacy information, beacons advertising either intelligent environments or their services must be complete and accurate. To avoid a malicious entity from spoofing an intelligent environment’s beacon to collect user information (when users unwittingly connect to it instead of the real environment) the intelligent environment’s beacon should be signed by a certification authority and the result stored on a local register with which the beacon’s signature can be compared.

6.2.2.1 User Register

The User Register broadcasts the existence of the intelligent environment using mDNS. These broadcasts provide information on the environment, and are identified by the user’s Persona Manager that manages the user’s connection to any available intelligent environments. Given that a particular environment might have multiple intelligent environments providing services to the area, the information provided by the User Register’s broadcast could be used by the user to determine which environment they would like to connect to. Information included in this broadcast includes a description of the intelligent environment’s purpose, a public key to allow the exchange of a unique session key (in absence of a Kerberos server managing session keys within the environment), links to the environment’s privacy policies and ownership details (refer to section 5.3.1) and a description of any information collection using traditional or ubiquitous computing technologies.

The User Register advertises the intelligent environment to its physical environment using mDNS messages. These beacons follow the `environment:environment_type:environmentname://hostname` format, which describes the type of environment, its name and hosted location. For example, a local university intelligent environment might look like `environment:public:SUN_Campus://localhost`. This format follows the standard method of describing available resources using mDNS messages (Cheshire & Steinberg, 2006). Each environment descriptor can efficiently be stored in an XML format (see Figure 14), and the user’s mobile device would collect these beacons and create an interface to access them on the user’s mobile device.
Figure 14: Sample Intelligent Environment Location Tag

Figure 14 describes the beacon sent out by each intelligent environment to inform potential users about their owners and information collection activities. Included in this broadcast are links to the environment's privacy policies, information collection descriptions (especially noting the sensor usage within the environment), relevant privacy and data storage legislation covering the area and links to the environment's public key (which is used in the event of no Kerberos server being available to securely manage communication within the environment). This information should be automatically parsed by the user's mobile device, which would react to the information according to the user's privacy and interaction preferences. For example, a user might forbid interaction with any environment that uses biometric sensors or has a lengthy information storage policy. The user’s mobile device might then provide a warning (either passive or active) to the user about the environment, or in extreme cases might reject the environment and not allow the user to connect at all.

Users entering such an environment would see the intelligent environment appear on their Persona Manager interface, and then users could choose to connect to the environment using a default or specifically selected Persona. This connection involves the user’s mobile device creating a randomly generated MAC address and IP address to interact with the environment’s User Register. This allows the user to obscure their machine’s identity, allowing them to avoid privacy threatening logging and tracking of the user’s mobile device across this or multiple intelligent environments. Use of random MAC addressing in a wireless LAN is demonstrated in (Gruteser & Grunwald, 2005).

Once this connection to the wireless network is achieved, the Persona Manager on the user’s mobile device provides the appropriate persona and contact information to the User Register, encrypted using the intelligent environment’s public key. This initial connection is used to exchange a symmetrical session key for the secure exchange of information while the user remains within the intelligent environment. The contact information exchanged with the environment includes the user’s Identity Broker’s address.
and public key to allow the secure exchange of information requests to their Personal Domain. Details of the personae used to share information with the User Register are provided in section 6.2.1.1, whilst a complete description of the contact information exchanged is described in Figure 15.

After the user’s persona and contact information has been received, the User Register stores this information in the User Details database. This information is used to populate the list of users sent to the user’s User Manager upon connection with the environment. A user can then request more information on any user on the list from their Personal Domain. Requests for more information are forwarded by the User Register to the User Information Requester, and this process is described in section 6.2.2.3. This method provides users with a secure method of interacting anonymously with the intelligent environment whilst still retaining some ability to interact with other users within the environment. Further details of the Identity Manager, the Personal Domain and their uses are described in sections 6.2.3 and 6.2.4.

6.2.2.2 User Details Database

The User Details database stores the user’s persona and communication information passed to the User Register. The user’s persona information is shared with other users that connect to the intelligent environment. This public information is designed to promote interaction between users and provide a private and secure method of exchanging information. The user’s communication information allows this exchange by storing the user’s Identity Manager’s contact information and their local network IP address. The information that could potentially be stored within this database is described in Figure 15.

<table>
<thead>
<tr>
<th>User</th>
<th>User Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID*</td>
<td>User ID*</td>
</tr>
<tr>
<td>Name</td>
<td>Identity Manager Address (URL/IP Address)</td>
</tr>
<tr>
<td>Picture</td>
<td>Identity Manager Number (encrypted using IdM Public Key)</td>
</tr>
<tr>
<td>Alias</td>
<td>Identity Manager’s Public Key</td>
</tr>
<tr>
<td>Personal Details (Interests, Public message etc.)</td>
<td>User Environment Locator (IP Address/MAC Address)</td>
</tr>
<tr>
<td>Contact Details (e.g. Public Email Address)</td>
<td></td>
</tr>
</tbody>
</table>

Figure 15: User Details Database

The public information stored within the **User** record element includes a unique User ID and all information included in the persona provided by the user’s Persona Manager. This information would normally be used to promote interaction with strangers or to allow users’ friends to recognise them, but it is anticipated that many other information sharing uses might be found for this public space. For example, it is likely that some fields might be used to share personally created art (e.g. a creative photo), or that a description field might be used to sell goods or advertise community events. The fact that this information is released solely by its owner allows users the option of representing themselves anonymously if they so desire.

The **User Connections** record element stores the information necessary to create a secure, anonymous link to the user’s Personal Domain. This includes
the user’s Identity Manager’s address and account number (encrypted along with the current date and time, using the Identity Manager’s Public Key), the Identity Manager’s Public Key (to allow any requests to be encrypted before transmission) and the user’s current network address to identify the user within this session. This information is accessed by the User Information Requester when creating a new information request to be sent to the user’s Identity Manager. The user’s Identity Manager’s public key is provided to all other users along with their public information to allow any information requests to be encrypted, preventing the intelligent environment from determining the contents of such a request.

To ensure maximum user privacy, these information records are designed to be discarded when the user leaves the environment. However, users will often have no evidence of this data expiration, beyond trusting the intelligent environment’s privacy policies, which may or may not be accurate. Information should therefore only be shared if it is either public (e.g. the user’s personae), encrypted using a third party’s public key (e.g. their Identity Manager’s account number or personal information attached to a ‘more information’ request), or not linkable to the user (e.g. through tracking their MAC/IP addresses). The Identity Manager’s account number is also encrypted along with the current date and time to prevent the encrypted number being compared with other previously supplied numbers in an effort to match two user interactions together. More security can be found by blind routing the information to its destination in the manner described by the Gaia OS (Campbell et al., 2002).

Users may require training or guidance on what information should or should not be placed in public forums to help improve their anonymity or reduce the risk of being tracked across multiple sessions. This is perhaps something that many people will want to occur as they define themselves in the intelligent environment space, and is probably similar to the personae that users adopt when interacting on Internet chat sites. It may also form the basis for the casual community interaction described in sections 2.2.3 and 5.2.1. Work is also required to ensure privacy policies are accurate, either through the clear identification of the companies behind an environment, to maintain public accountability, or through an independent certification (this is similar to the audits conducted on online gaming sites).

6.2.2.3 User Information Requester

The User Information Requester is used to gather more information about a user from their Identity Manager and subsequently from their Personal Domain. These information requests are made on behalf of other users and environmental entities. Responses to these requests can be either routed back from the Identity Manager through the intelligent environment, or could provide a real-time connection for both users, depending on the nature of the request. Any response made to the user will always be secured by encrypting the response using the user’s public key, which is sent with the information request along with their current IP address if a real-time link is required.
Requests sent through the intelligent environment are encrypted with the destination’s public key (the user’s Identity Manager’s public key).

Requests sent to the user’s personal domain could have a multitude of purposes. Simple requests for information could be made by a user (or their device) when seeking to confirm the identity of another intelligent environment user. Given enough of the first user’s personal information, the second user’s Personal Domain could recognise the user and confirm their identity in return. Other more specific information requests could seek location information, e.g. when attempting to locate a friend or family member, attempting a VoIP or instant messenger connection, or requesting a photo so the user can be recognised.

The use of an always-on, user-controlled third-party Personal Domain allows information requests to be served by a user-controlled entity that is not the user’s mobile device. This reduces the computational burden on potentially lightweight mobile interfaces, and allows user information to be accessed when the user is offline. The use of Personal Domains could also allow users to connect to their friends directly from within any intelligent environment or network environment. Users that have previously shared their Identity Managers’ addresses (and their public keys to allow the initial exchange of a session key) could access each other’s public information and request location or communication information. The Identity Manager provides a layer of obfuscation to prevent the mining of personal domain locations (see section 6.2.3 for more information).

An information request is made by a user, (A), by selecting a particular user, (B), from the list maintained by their mobile device’s User Manager. The mobile device creates a ‘more information’ request, and connects to the User Register to request user B’s Identity Manager’s public key using their temporary User ID. The User Register accesses this information from the User Details Database and provides it to user A’s User Manager, which uses the public key to encrypt the entire information request. This request is then forwarded via the User Register to the User Information Requester.

When a request for more information is received, the User Information Requester accepts the information request and accesses the user’s Identity Manager account number and address from the User Details Database. The User Information Requester then attaches the (encrypted) user’s Identity Manager account number to the beginning of the request and posts the information request to the Identity Manager’s address. This simple method of information transportation prevents the intelligent environment from having access to the personal information within the information request and alleviates the need for the environment to complete any encryption. This reduces the computational complexity required to run the User Register, an advantageous requirement given the relatively simple computational devices found in ubiquitous computing environments, and the potential for large numbers of users to be connected to the user register at any one time.
6.2.2.4 Privacy Threats and Analysis

Threats to users’ privacy could include the monitoring of users’ wireless communication with the environment, collection of the information users provide to the environment, and the use of sensor information to record information about the user that they do not wish to provide to the intelligent environment. Interaction with an intelligent environment’s user register is completely user initiated. This provides the user with the ability to determine if and how they wish to interact with an intelligent environment and what information that they wish to provide about themselves.

Intelligent environments (and their user registers) are not inherently trusted, and could be provided by a malicious entity. Therefore users cannot trust any information provided to the intelligent environment on a private basis will remain so (no matter the privacy assurances given or regulatory framework responsible). Users must therefore develop their own strategies to protect their privacy in the event of such a breach. For example, the information provided should be generic enough that it could not be used to recognise the user. But it is expected that many users will provide recognisable information about themselves (as they do on the Internet today). Furthermore users are likely to develop their own uses for publicly-available information as intelligent environments become a commonly used interaction tool.

The non-public information provided to the intelligent environment includes the user’s Identity Manager’s address and an encrypted account number. To counter the risk of their identity account information being stored by a malicious intelligent environment, a blind reference to the identity manager is used (providing no personal information). Users will also use multiple IdM accounts (and encrypt the information with the current date and time) to prevent the linking of a user’s visits. The use of random unique connection IDs when communicating with the intelligent environments also prevents these connections from being made. Further discussion on the threats to users surrounding the use of the User Register is discussed in section 7.2.1.

6.2.3 Identity Manager

The Identity Manager (IdM) provides a secure connection to the user’s Personal Domain without exposing the domain’s address to other users or the intelligent environment, or exposing users to data mining or traffic analysis attacks on their privacy. The Identity Manager provides an anonymous method of accessing a user’s personal domain or other services that the user may want to access anonymously. When the user connects with the user register of an intelligent environment, they can provide their IdM address, encrypted IdM Number and IdM public key instead of their direct personal domain address.

When another user requests information about the original user, they make an information request to the user register encrypted by the IdM public key. The user register then forwards this information to the identity manager, which then decrypts the IdM number and information request details. This prevents an intelligent environment from collecting information on the
location of a personal domain and the contents of the original information request. This further prevents the environment from applying that information to other details collected about the user while they interact with the intelligent environment and its services.

The use of a centralised data store for the exchange of identity information (and interaction preferences) is preferred over its storage on the user's mobile device. The personal domain provides a persistent storage of information that can be queried without concern for the user's mobile device (and any battery or connectivity constraints) (see section 5.2.5). Each Identity Manager account should have multiple reference numbers (that the user can provide to the intelligent environment) to eliminate the risk of an encrypted account number being matched with a prior identity manager reference, thus matching the user to a previous interaction history or public persona. Users should also use a number of identity managers that refer to the same personal domain, especially when interacting with environments that might have limited users using the same IdM as the user.

The Identity Manager is comprised of the Identity Manager Connection, which receives information requests, the Persona Requester, which forwards these requests to the user’s Personal Domain, and the ID Management Database, which stores the Identity Manager accounts containing the user's Personal Domain address and its public key. The Identity Manager's communication with other elements of the intelligent environment is described in Figure 13. These components are described below.

6.2.3.1 Identity Manager Connection

The Identity Manager Connection accepts information requests submitted to the Identity Manager (see Information Flow C in Figure 13) and passes these requests to the Persona Requester. All information requests are sent encrypted using the Identity Manager’s public key on the requester’s mobile device. These messages are then decrypted by the Identity Manager before being forwarded (encrypted with the Personal Domain’s public key) to their ultimate destination. The Identity Manager Connection then accepts the request’s response from the Persona Requester (originating from the user’s Personal Domain) and returns the result (securely) to the user's mobile device (see Information Flow E in Figure 13).

Information requests contain all the information required to interact with the user’s personal domain and to allow the return communication with the inquirer. Prior to making the information request, the user’s mobile device encrypts the request information using the Identity Manager's public key. This information request is then forwarded to the intelligent environment’s user register, which adds the destination Identity Manager’s ID Number to the request. The destination ID Number was provided by the original user (that the request is about) already encrypted using the identity manager’s public key. This number is used as a reference number to determine which account to access, and each user would have multiple ID numbers referring to a particular identity account. The creation of these information requests is discussed in section 6.2.2.3.
This use of a third party to securely relay sensitive personal information is comparable to the Mist Routers described in the Gaia OS (Campbell et al., 2002). This implementation demonstrates the use of multiple public key encryptions to secure the message and its ultimate destination. This message security allows users to maintain their information privacy while sharing information across an intelligent environment or wireless network. This blind relay method is also used to route information requests to the user’s Identity Broker, described in section 6.2.7, but the location of the Identity Broker is not disguised, because it is essential in order to have confidence in the results that it provides.

6.2.3.2 Persona Requester

The Persona Requester forwards information requests made to the Identity Manager Connection directly to the user’s Personal Domain (refer to Information Flow D in Figure 13). To accomplish this, the Persona Requester provides the IdM ID Number to the ID Management Database and receives the user’s Personal Domain address and public key. The Persona Requester then encrypts the information request using the Personal Domain’s public key and sends this request to the user’s Personal Domain. Once the request is sent the returned result, if any, is passed back to the Identity Manager Connection entity to be returned to the request originator. Information requests can include a different return address to route the results directly back to the requester. This would particularly be the case when the information request is for a direct communication channel, like a VoIP call or instant messenger chat connection.

6.2.3.3 ID Management Database

The ID Management database stores all the information contained within the Identity Management account created by the user to allow the private routing of information to their Personal Domain. This information (described in Figure 16) includes the user’s Name and Account ID, their Personal Domain address and public key, and the Identity Manager’s identity numbers (IdM ID#) that are used to reference the user’s account. This information is referenced by the Identity Manager Connection and Persona Requester entities described in the previous sections.

<table>
<thead>
<tr>
<th>IdM Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account ID*</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Personal Domain Address</td>
</tr>
<tr>
<td>Personal Domain Public Key</td>
</tr>
<tr>
<td>IdM ID#</td>
</tr>
</tbody>
</table>

Figure 16: ID Management Database

The ID Management database contains many IdM ID numbers for each IdM account. This allows the user to maintain a large set of reference numbers that can be exchanged (normally encrypted) with other users or intelligent environments. Users can then provide completely different IdM ID numbers each time they interact with an intelligent environment, without the environment being able to compare the Hash values of previously submitted
numbers. This provides the users with additional protection in the event that an intelligent environment stores submitted user information in order to compare and link users between visits. Additional security can also be gained by including the current time and date in the encrypted packet, preventing the same number from being recognised when used in multiple service requests.

**6.2.3.4 Privacy Threats and Analysis**

The identity manager provides a blind connection to the user’s personal domain for information requests and service access. This blind relay prevents intelligent environments from gathering the user’s Personal Domain’s address, which, as a unique identifier, could be used to recognise the user in the future. All communication between the intelligent environment, the Identity Manager and the Personal Domain is encrypted to prevent eavesdropping. The user could obtain further privacy protection by maintaining multiple Identity Manager accounts with multiple Identity Manager entities. These accounts could then be used randomly to ensure that the same Identity Manager is not routinely used, thus denying the intelligent environment the only information that could conceivably be connected to a user’s interactions.

**6.2.4 Personal Domain**

A Personal Domain is a user-controlled repository of information that can be used to store user information and to provide this information to inquiring third parties (in accordance with the user’s privacy preferences). This allows the user to have a permanent presence in the ubiquitous computing world, allows them to share information without requiring third parties to connect to their handheld device (a potential breach of privacy) and relieves the computational load on the user’s handheld device. This will allow users to interact with intelligent environments using simpler, smaller devices, and will possibly lead the way for other forms of interaction with the intelligent environment, for example biometric user recognition. The case for using a centralised data store versus storing the information on the user’s mobile device is discussed in section 5.2.5.

A user’s Personal Domain acts on behalf of a user accepting information requests and managing the user’s contact information. A Personal Domain provides information about the user to third parties based upon the requester’s identity and the user’s privacy preferences. Information regarding the user may be freely given once a previous connection is established, for example, the inquirer is on a ‘friends list’, or distributed based upon any number of privacy conditions relating to the information requested and the user’s current context. The Personal Domain also manages personal information, such as the user’s physical location or network address, which could be used to locate or connect to a user’s mobile device. This permanent, user-controlled information repository would be especially useful in providing always-available information services and maintaining contact between different groups of people (e.g. a user’s urban tribe or work colleges). This could then be used to provide communication services, e.g. VoIP or IM, or to
integrate with other location-based services, e.g. LocServ (Myles, Friday & Davies, 2003).

The user’s personal domain accepts information requests and provides the appropriate personal information in line with the user’s privacy preferences. These requests are normally routed through the user’s Identity Manager, described in section 6.2.3, but anyone with the domain’s address can send requests to the Personal Domain directly. Requests are encrypted using the Personal Domain’s public key and contain a return address and public key for encrypting the response. The user’s Personal Domain should store all information requests to allow users to see interaction histories, which could be useful for tailoring what information is provided to what type of users.

A typical information request, described as Information Flow D in Figure 13, could be used to identify more information about an environment’s users, help recognise friends in the environment or request other communication connections (e.g. VoIP or IM). A permanent online presence via which the user could be contacted would further improve users’ management of online services and help maintain their connectedness to their urban tribe. The Personal Domain’s Privacy Manager evaluates the request and provides information in accordance with the users’ stated privacy preferences, stored in the Persona Database.

6.2.4.1 Privacy Manager

The Privacy Manager accepts information requests on the user’s behalf and responds according to privacy policies predefined by the user. To do this, the Privacy Manager examines the information provided with the information request, loads up the appropriate privacy preferences (stored in the Persona Database) and evaluates what information or user persona to return. Information requests follow the schema: {[[User Information], Request Type / Information, [Return Address Information]]}. User information would most usefully be exchanged using a common persona modelling language, e.g. the XML-based ‘Personis’ modelling language (Kay, Kummerfeld & Lauder, 2002) described in sections 2.3.4 and 6.2.1.1. The return address information provides the return IP address and public key used to encrypt the response for transmission back to the inquirer. Information request results either return a persona describing the Personal Domain’s owner, or an IP address to allow two parties to establish a synchronous communication connection.

Consider the example of a Personal Domain being used to connect two friends (Daniel, User A; Gloria, User B) using an instant message (IM) connection. As they are friends, user A has user B’s Personal Domain address, so he sends the request directly to the Personal Domain. However, if desired, this request could as easily be routed through the user’s Identity Manager. User A sends the following information request to the Personal Domain:

Request: {[[Daniel, ‘Email’, ‘Personal Domain’], 2 (IM Connection Request), [Return Address (IP Address, Public Key)]]}

Daniel’s request identifies him, using his name, email and Personal Domain’s address, and asks for an IM response. Gloria’s Personal Domain receives the request and loads her personal privacy preferences from the Persona
Database (described below). Gloria’s privacy policy indicates she only accepts these messages from her friends, and only if she is currently online (either in the same environment as Daniel, or in another environment where she is connected to her Personal Domain). Daniel is recognised by Gloria’s Privacy Manager, using his email address, as being one of her ‘Contacts’, and an IM connection is approved. This connection is made by sending Daniel’s mobile device the following information encrypted using his public key:

Result: {'return address’ (Gloria’s IP Address and Port Number)}

If in the above example Daniel’s request was for more information, a persona describing an aspect of Gloria’s identity would be returned. If Daniel and Gloria weren’t friends, then her personal domain would have determined, based upon the information he shared in the request, which persona to return. For example, her privacy preferences might state that, because he is providing his email address and Personal Domain address, she will also share this information. The exact nature and influences on this process of developing and improving the use of privacy preferences for user information sharing is ultimately outside the scope of this study, as it requires an extensive longitudinal investigation of an intelligent environment that allows this kind of user interaction. However, this evaluation would be usefully augmented using a Trust or Reputation system that could be applied to all elements of the intelligent environment (e.g. users, intelligent environment owners, services etc.). These systems would provide additional information to help users to determine risks of information exchanges to their privacy and could be automated into the user’s privacy preferences. Trust and reputation systems are examined in section 2.4.6, and their addition to the SPACE architecture is discussed in section 6.5.3.

6.2.4.2 Persona Database

The Persona Database contains all information required in the evaluation of information requests made to the Personal Domain. The database contains information on the user, including their name, age, location (if known) and the user’s privacy policies. The user's privacy policies describe how the Personal Domain should release information or respond to information requests. The Personal Domain should also store a record of information requests to provide user feedback on how their Personal Domain is being accessed. Information stored within this database is described in Figure 17.

<table>
<thead>
<tr>
<th>Personae</th>
<th>Contacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persona ID*</td>
<td>Contact ID*</td>
</tr>
<tr>
<td>Persona Name</td>
<td>Last Name</td>
</tr>
<tr>
<td>Persona Description</td>
<td>First Name</td>
</tr>
<tr>
<td>Last Name</td>
<td>Age</td>
</tr>
<tr>
<td>First Name</td>
<td>Alias</td>
</tr>
<tr>
<td>Age</td>
<td>Email Address</td>
</tr>
<tr>
<td>Alias</td>
<td>Public Domain</td>
</tr>
<tr>
<td>Homepage</td>
<td>Public Key</td>
</tr>
<tr>
<td></td>
<td>Information Access</td>
</tr>
</tbody>
</table>
Chapter Six: A Solution for Privacy in Ubiquitous Computing

Contact Information
Contact ID*
Last Name
First Name
Email Address
Address

Privacy Policies
Policy ID*
Policy Name
Policy Description
Information Required

Location
Location ID*
Date/Time Stamp
Location Name
Network Location (IP#)
GPS Coordinates
Activity

Request History
Request Number*
Request Type
Information Requested
Requestor Name/Contact ID
Request Return IP Address
Request Result

Figure 17: Personal Domain’s Persona Database

The Personae record element stores the different Personae used to provide information on different aspects of the user’s identity for different purposes. For example, one persona might be used to share information with friends, while another might be used for anonymous information requests. The Contact Information record element maintains the user’s contact information, while the Location record element allows the user to maintain (if desired) a centralised set of location information that could be used to provide their location to friends and family, or provide the ability for a third-party service to share their information for them. Information requests are stored in the Request History record element.

The Contacts record element describes user contacts that have previously been imported or have requested information from the Personal Domain. This information store maintains an ‘Information Access’ field that allows the user to define the access that a contact has to their information. A simple scheme might set levels from 1-3, with user information (personae) available at level 2 and location information from level 3. A more complex scheme would most likely set different access rules to take into account the time of day, the user’s current context or a wide range of other variables. This contacts information could also usefully be integrated with other contact lists, for example, email or phone address books.

The Privacy Policies record element describes the different rules that the user has set regarding the sharing of their information. These rules might concern the information required from the requester before providing a certain persona, the time of day or activities that the user is currently involved in (if this can be determined by location record element or by other means) or whether the requester is part of the Contacts record element (and what their information access level is). The design and use of Privacy Preferences within ubiquitous computing is discussed in section 2.4.2.

6.2.4.3 Privacy Threats and Analysis

The Personal Domain has the ability to store all of the user’s personal information to allow distributed service management secure distribution of user information. But having this information in one place could make an
attractive target for malicious entities. Beyond access to the user’s unsecured mobile device, unrestricted access to the Personal Domain remains the greatest security risk in the SPACE architecture. The SPACE architecture mitigates this risk by locking down the methods of interacting with the Personal Domain, allowing only specific service connections direct to the domain and limiting information requests to those routed the user’s Identity Manager.

Direct connections made from the user’s mobile device to their personal domain (e.g. for access to information backups and for connections to communication services) use the blind routing system developed for use in the Gaia OS that disguised the packet’s destination. This, combined with the encryption used when communicating with the user’s personal domain, ensures that the contents and destination of any communication from the user is secured from any eavesdroppers. The personal domain also allows basic information requests to be served by an external entity. This prevents observant onlookers, or wireless communication packet sniffers, from easily linking a user register’s entry to the users within the physical environment.

Information request responses will often be routed directly back to the requester via the intelligent environment’s Internet access. But occasionally the response will be a discrete packet that is passed back via the intelligent environment’s server. In either case, the response is encrypted using the requestor’s public key, which effectively prevents anyone from gathering this information through malicious means. It is of course possible for another user in the environment to gather as much information as they can from the user’s Personal Domain for malicious reasons. The user’s privacy preferences that manage the responses from the Personal Domain should be sophisticated enough to avoid giving information to strangers that could negatively impact on their privacy, and users could at any time prevent any information from being returned from their Personal Domain. Further discussion on the threats to users surrounding the different types of identity brokerage is discussed in section 7.2.3.

6.2.5 Service Provider

The Service Provider manages access to the intelligent environment’s services. This entity is not only responsible for service delivery, but confirms the rights of the user to use the service and can perform or request confirmation of identity from a third party (e.g. via a signed user information template or through access to the identity broker). Services are provided within an intelligent environment by broadcasting a service’s availability across the environment’s wireless network using a Service Beacon. These services are then individually detected by the user’s mobile device and accessed via their Services Manager. The Service Provider, and its communication with other elements of the intelligent environment, is described in Figure 13.

Services can be classified as either Environmental or Global services, depending on their purpose and intended audience. Global services provide support services to all users of the ubiquitous computing infrastructure.
Environmental services support users within the environment and reject service calls from outside the environment. This localisation of service delivery helps prevent information from leaking across a natural border of privacy. For example, a service might be restricted to sharing users’ location details only with entities within the current environment. This prevents unintended breaches of privacy and reduces the chance of external denial of service attacks on the service provider from succeeding.

The use of a decentralised broadcast delivery scheme reduces the need for a central entity to manage the services, improves scalability and allows new services to be added to the environment without the need to negotiate with the environment’s owners. This service delivery method also prevents the environment from logging all service access, something that is possible when using a central service distribution point (like that used in iCrafter (Ponnekanti et al., 2001)). Decentralised service delivery does not allow a centralised entity to combine environmental services ahead of time and provide interaction patterns that can be used to create interfaces for new services, but service providers could use standard interfaces (or service aggregators) when developing their service to ensure ease of use.

This decentralised approach highlights the need for independent entities to validate the identity of the individual services and the users that can access them. Services must have an efficient method of proving their identity to prevent other users or service providers from faking existing services for malicious purposes. A service’s identity information is included in the Service Beacon that advertises the services to the environment’s inhabitants. Users must also be able to confirm their identity, via a signed user information template or through access to the identity broker, to allow services a method of controlling access to their service. This access control is provided by the service provider’s Authorisation Entity, described in section 6.2.5.3.

Any user interacting with an intelligent environment’s services is faced with varying degrees of the invisibility problem, in which information relevant to the user is lost amongst the potentially vast stream of public information and available intelligent environment services. Intelligent environments must provide a method of personalising this information that allows users to maintain their privacy and information security. This personalisation can occur on the user’s mobile device or on a central server, possibly the same server that provides the intelligent environment’s service. The goals of allowing users to maintain control of their personal information suggests the personalisation would be best on the user’s mobile device, as demonstrated in the BlueStar location-aware information guide (Quigley et al., 2004) and in our own research in section 4.3.

The trade-off with this form of personalisation is the need to transfer more information than is necessary to the user’s mobile device and the additional drain on the available wireless bandwidth. Given that ubiquitous computing is a relatively new field, and the fact that wide-scale implementation and experimentation of these environments is still several years off, we suggest that this bandwidth problem will be addressed by the improving technical capabilities of wireless communications hardware and mobile devices. This
problem (and solution) is less of a design issue than surrendering control of a user’s personalisation information to potentially untrustworthy systems. Personalisation of services within intelligent environments is discussed in section 2.3.5, and a solution for maintaining user privacy whilst interacting with personalisable services is discussed in section 6.5.2.

6.2.5.1 Service Beacon

The Service Beacon broadcasts the availability of a service within the intelligent environment to all users using multicast DNS (mDNS), shown as Information Flow G in Figure 13. Services are described using the service: servicetype:servicename://hostname format, which describes the type of service, its name and hosted location. For example, the service instance name of a local directory service providing directions around campus could look like service:directions:SUN_Campus://hostname. The service names follow the naming conventions for describing services using mDNS messages (Cheshire & Steinberg, 2006). Service Beacons are used in the iCrafter (Ponnekanti et al., 2001) and Privacy Aware System (PAWS) (Langheinrich, 2002) intelligent environments to share privacy-related information with potential users of their services.

Environmental services (see section 5.2.2) are designed to be only locally accessible, and thus their names end in the .local designation. This standard notation prevents the mDNS message from being forwarded beyond the local-link network (Cheshire & Steinberg, 2006). Each service interface can be efficiently stored in an XML format (see Figure 18), and the user’s mobile device would collect these and combine them into a general services interface.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<service>
  <TITLE>State UniversityNorthern Campus Directions </TITLE>
  <TYPE> Directions </TYPE>
  <ACCESS><a href="http://localhost/directions/">
    [Access Directions]</a></ACCESS>
  <OWNER>State University, IE #102 </OWNER>
  <POLICIES> http://localhost/privacy/ </POLICIES>
  <POLICIES> http://localhost/legislation/ </POLICIES>
  <INTERFACE> http://externalhost/int-template/ </INTERFACE>
  <PREFERENCES> Student </PREFERENCES>
</service>
```

**Figure 18: Sample Service Interface Tags**

The distributed multicast broadcast model used to advertise and access services means that any entity within the intelligent environment could potentially offer a service. The usefulness of these services is only limited by the designer’s imagination, and many services could be offered by users with unique skills, hardware or access to information. This ability to provide services in an ad hoc manner does, however, mean that a method of identifying the service provider and their policies of information reuse must be available. This information would be provided in the service beacon broadcast, and where possible should be in a machine-readable form to enable the user’s mobile device to evaluate the policies alongside the user’s
privacy preferences (e.g. like those used in the PAWS system (Langheinrich, 2002)).

Additional information can be added to the broadcast to enable users to make better use of the described services. For example, the ‘Preferences’ tag shown in Figure 18 could be used by the users’ mobile devices to select services appropriate to their interests. The ‘Legislation’ tag is used to identify any legislation in the immediate area that might contravene the user’s privacy preferences. Information on the service’s owner and its information sharing policies should also be shared in this manner, providing users with the information they require to make informed decisions upon what information they would like to share with the service. This requirement was identified in the user studies in chapter four and is summarised in section 5.3.1.

The Service Beacons broadcast could also contain the information required to access the service (whether it be confirmation of the user’s age, service preferences or real identity), or any interaction template that can be used to access the service or build the user interface. (Information templates are described in section 6.2.6.) Users can access a service by sending their request, and user information, to the service’s IP address (see Information Flow I). This information request is accepted by the Service Provider entity. Once again, as the beacon is used as an initial source of privacy information, beacons advertising intelligent environment services must be complete and accurate.

6.2.5.2 Service Provider

This component provides personalised services delivery based upon the persona provided by the user (or their mobile device). The persona can provide proof of access in conjunction with the authorising entity (see the next section), or a more sophisticated persona might contain all the information required to deliver a service. For example, this might return all new news articles based upon the given keywords; or validate access and provide a daily access code for all doors within a particular building based upon the provided access codes. These types of service calls could potentially be used to identify the user, so user care and adequate feedback on the interaction parameters would be required.

The Service Provider’s location (IP Address) and contents are described by the Service Beacon that publishes information on the availability of the service using mDNS. The Service Provider accepts service requests (see Information Flow I) sent by the user’s mobile device, or user’s inputs from the service interface described by the service beacon (refer to Figure 18). This allows for manual (by the user accessing the service’s interface) or automatic service interaction (with service requests being created by the user’s mobile device in accordance with the user’s preference). The actual service provided by the Service Provider is not of as much interest here as the information exchanged and the authorisation process that occurs when interacting with an information service, but potential services are described in section 5.2.2.
Information Flow I contains the user’s choice of an identity broker account or digital template that is used to confirm the user’s identity. An identity broker’s information also contains a public key with which all requests to the broker are encrypted. The user’s identity broker account number is also encrypted, with the local time and date, to prevent the storage of this information for future comparison between uses (which can lead to extensive user information being compiled and applied to the user in future interactions). The use of a digital template requires the Service Provider to either parse the template and determine for itself what information is represented, or contact the template’s issuer for a template guide to aid in its parsing.

Upon request, the Service Provider’s Service Connection provides information on the signing entity, on the template’s location and on its format (see Information Flow F). This allows the Service Provider to easily parse the template to extract the user’s information and provide information to the authorisation entity about the Information Service Provider that can be used in determining the levels of trust applied to the information template. The use of digitally signed templates is described in section 6.2.6, while the trust determinations made about the signing entity are described in section 2.4.5.1.

6.2.5.3 Authorisation Entity
The authorisation entity is used to authorise users of a particular service, either by examining their signed information (from an Information Service Provider), by matching user details with those in the Services Database, or by confirming required information (e.g. name, age, financial resources, etc.) via interaction with an Identity Broker. The type of identity authentication required will depend upon the level of trust in the shared information that is required by the service provider. This section describes how each of these identity authentications occurs.

The most common identity authentication relies on internal user accounts maintained by the service provider. These will be used for services that do not require formalised identity authentication, e.g. an account maintaining the user’s information searching preferences, or for service accounts where the user’s identity is only verified upon the accounts creation. This authentication attempts to match user-supplied information, e.g. name or account number, with the information stored within the service provider’s Service Database. Users interacting with an environment’s service using ‘User Selected Pseudonyms’ (see section 6.5.2) would fall into this category of identity authentication.

Some services will often require more formal confirmation of a user’s identity. This is accomplished by confirming information provided by the user with a trusted third party, using either their Identity Broker or by accepting a signed digital template containing the user’s personal information. To confirm the user’s information using an Identity Broker, the Authorisation Entity makes the following request to the Identity Broker identified by the user when requesting access to the service (refer to Information Flow J in Figure 13):

Identity Confirmation Request (to IdB location (IP#); encrypted: IdB Pub Key): {IdB #, request type (send=0, confirm=1), [information to confirm], service location (IP#), servers Pub Key}
Identity Confirmation Response (to service location (IP#); encrypted: Service’s Pub Key): {Confirmation (True=1, False=0), [requested information]}

The intelligent environment’s Kerberos server is used for exchanging one-time session keys for this communication exchange, but both entities’ public keys are present for encrypted communication in its absence. Without the Kerberos server, the information request is sent encrypted using the Identity Broker’s public key, provided with the service request (in Information Flow I), and returned using the Service Provider’s public key. The Identity Broker’s account number is also encrypted (using the Identity Broker’s public key) to prevent the collection of information about the user by the service provider or anyone monitoring the intelligent environment. This number is encrypted along with the time and date to prevent this information being compared between sessions. (Unless the date and time is included, the encrypted Identity Broker number would always be the same, and could be matched between sessions.) The confirmation of a user’s information using an Identity Broker is described in section 6.2.7.

The usefulness of signed digital templates will vary greatly between intelligent environments. An environment developed with a specific audience in mind might also have a trust relationship with the users. For example, a university-owned intelligent environment might accept signed digital personae from the university allowing students to be easily, and anonymously, recognised by other users. When using a signed information template to confirm parts of the user’s identity, the Authorisation Entity must determine the trustworthiness of the signed template based upon previous experience and its relationship with the provider. The use of information templates allows the identity authentication process to be conducted within the environment, which would be useful for stand-alone systems, particularly in areas of high security. The use of these signed information templates is discussed in section 6.2.6.

6.2.5.4 Service Database

The Service Database contains any information that the intelligent environment’s Service Provider requires to deliver its services. This includes details on the available services, required authorisation, user accounts and interaction histories, current environmental information and any relevant information-sharing policies and service ownership. The information is maintained in separate record elements to allow the control of information by its owners. The information and its primary keys are described in Figure 19.

<table>
<thead>
<tr>
<th>Service Authorisation</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ID*</td>
<td>Service ID*</td>
</tr>
<tr>
<td>User ID (any authorised users)</td>
<td>Service Name</td>
</tr>
<tr>
<td>Authorisation Rules (e.g. ripple down rules)</td>
<td>Service Description</td>
</tr>
<tr>
<td></td>
<td>Service Interface Tag (Location IP Address)</td>
</tr>
</tbody>
</table>
The service provider must have trusted computing components to allow the secure storage of information within the ‘Service Users’ database. This allows users to encrypt personal information within an intelligent environment with the expectation that this information will only be available to the user and not to the environment in their absence. (Access to this information follows the format described in section 5.2.5.1). The ‘Interaction Histories’ should be available to the intelligent environment or the user, but they should not be available outside the intelligent environment (to avoid moving information outside natural borders of privacy). The ‘Interaction Summaries’ database contains anonymised interaction summaries that allow the environment to correlate information on service usage and share it across multiple intelligent environments or service providers without privacy concerns.

6.2.5.5 Privacy Threats and Analysis

Whilst services are the main driver for the development of intelligent environments, they also have the potential to be the main cause of users’ privacy concerns. Users will have to provide personal or preference information for most services, and this information could potentially be very sensitive (e.g. medical records or financial information). Users must therefore make a decision based upon their perceptions of the value of the service compared to the potential risks to their privacy if the personal information that must be exchanged is compromised. Service Beacons help users make this determination by providing them with information on the service’s owners, information collection and retention policies, and by providing links to any relevant privacy legislation.

Service providers have the same problems of physical accessibility that the User Register and all ubiquitous computing systems experience. Protecting the interaction histories stored within the service provider’s hardware is important. Hardware should be hardened against physical tampering, and trusted computing components should be used to authenticate that the service has not been tampered with. Trusted computing authentication could be used with a central database to further ensure that an expected service is not being spoofed by a malicious third party. Information exchanges with a service should also be encrypted using a shared session obtained from the intelligent environment’s user register, except when the service does not required encryption (for example when accessing non-sensitive information).
The final threat that users experience when interacting with service providers is the threat of subversive activities by the service itself. This threat includes the service storing, reusing and disseminating the user’s identity information, personal descriptions, interaction preferences and service usage histories. The dangers of the collection of identity information (including the user’s personal identity accounts: Identity Broker IDs, secured personal pseudonyms and Identity Management IDs) are described in the relevant sections on the workings of the identity structures. The threat of the collection and reuse of personal information is more difficult to frame.

Information collected about a user over time could be used to build up a profile that could be used for advertising or for more nefarious purposes. This profile could also be compiled by legitimate services, so the design of services also plays an important role. The SPACE architecture encourages the use of multiple user accounts for local services where personalisation is desired and anonymously when it is not. Local services should not allow information to pass to other environments, and users should set their interaction preferences to ignore services or environments without clear guidelines on information reuse. User education about the potential dangers of providing personal information will complement the many social campaigns about the dangers of exchanging information on the Internet.

The damage done by personal information stolen by a service provider is difficult to control. But the SPACE architecture has some measures in place to reduce both its occurrence and the damage done. Users entering an intelligent environment do so anonymously using a random unique ID, and as such cannot easily be recognised until they provide information that matches the stolen user profile. The use of identification and sensing technologies in intelligent environments is discouraged, but surveillance systems are unlikely to be removed due to their role in crime prevention. In these cases the intelligent environment should notify users they are under surveillance, allowing them to alter their behaviour or leave the environment if they so choose.

Service interaction is ultimately an assessment of benefits of interacting with a service against the potential risks to privacy that one takes by providing personal information for personalisation or service access purposes. But this ability to interact as the users choose (i.e. anonymously or using multiple interaction accounts) does not help when a user (as users consistently do) make interaction choices that seem to be contrary to their explicit privacy goals. This is countered by user education, effective feedback on information exchange, the enforcement of privacy laws and most importantly the ability to obtain timely feedback from peers on the dangers of using a particular service.

This feedback could be provided in an environmentally specific manner through the use of bulletin boards and user feedback forums. A more regimented feedback system could take the form of a trust and reputation system that is already used on online forums and has been suggested as potentially useful for ubiquitous computing environments (see section 2.4.6). The relative rating of the service provided by the trust and reputation network.
would then be displayed alongside the service in the user’s service interface, and would assist users in making their own risk determinations about using an environment’s services. The extension of the SPACE architecture to use trust and reputation systems is described in section 6.5.3.

6.2.6 Information Service Provider

An Information Service Provider (ISP) is an identity provider that provides environment-independent services to users within intelligent environments. These services should be either something that the intelligent environment cannot itself provide, like identity authentication, or a service that would be more efficiently provided using a distributed architecture. A good example is the sharing of information with an intelligent environment using a standard template, potentially with information that has been digitally signed to verify its issuer and the fact that it has not been altered since its issue. This structure was suggested by Hitchens, Kay and Kummerfeld (2004) to promote pseudo-anonymous, yet readable and verifiable information-sharing with intelligent environments, and is described in more detail in section 2.4.5.1.

Other services that this entity will provide include the management of user accounts containing user preferences that can be used across multiple intelligent environments, and reference services to support the coordination of users moving between multiple intelligent environments. For example, users might maintain their preferences for interacting with an advanced news search engine within an information template. This template would be used every time a user enters an environment that provides access to the news update services (e.g. Google news). Another template could be used to identify the user as a student to environments all over a particular city or state. The role that the Information Service Provider has within the intelligent environment infrastructure is described in Figure 13.

Users obtain a signed information template by providing the issuer with verifiable personal information that they wish to hold in their template. The issuer then verifies this information, either via an Identity Broker or by using a pre-existing relationship (e.g. prior enrolment at an education facility, passport, drivers licence, etc.), and digitally signs the information as true and correct. This file is then stored on the user’s mobile device and can be provided to a Service Provider when identification or service preferences are requested (see Information Flow H in Figure 13). The amount of trust (or the strength of the authentication) placed in identity information asserted using signed templates depends on the trust the service provider has in the ISP.

This identity authentication method attractive to users because they could potentially maintain a number of different signed templates for different interaction purposes. One could be used for anonymous interaction, another for accessing student-only resources, and a third might be used for shopping or other payment-based services. Using a number of ISPs to provide identity authentication could allow the user to assert identity information to a service provider or environment with a strong level of confidence, without needing to expose their identity broker or identity manager / personal domain. Examples of screenshots showing these templates in use are shown in Figure 24.
Using this third party to verify user information allows users to prove a verified identity to an intelligent environment without needing to supply an identity account, which could potentially be mined by the intelligent environment, and without requiring a real-time link to the identity broker. This transfers the trust relationship with the intelligent environment from the identity broker to the information service provider. A community-based or city-wide authority could be used to securely confirm the identity of anyone wishing to interact with a local intelligent environment without providing individual intelligent environments with their Identity Broker accounts.

6.2.6.1 Service Connection

The Services Connection entity provides the integration access point for ISPs within intelligent environments. This interface allows users and intelligent environments to access information on the details and layout of used information templates, and provides a reference database describing where each of the available templates is currently being accepted. This interface allows information templates to be integrated in real time into an intelligent environment as they are developed and become useful.

Users can use this interface to either create an information template (leveraging an existing relationship with the ISP or by providing an Identity Broker account) or to look up the templates in use within a given intelligent environment. User Information Templates are created by sending a request containing the information that the user would like to be digitally signed within the template to the ISP with a method of confirming this information. This could either be an Identity Broker account or an account number describing an existing relationship (e.g. student account number while interacting with a university). The templates could also be created in person, using traditional photo identification. Physical relationships can jump-start trust between entities, and this might be seen as more reliable than purely digital-based IDs.

All information exchanges with the ISP are encrypted, and the identity broker number is encrypted with the current time/date using the Identity Broker’s public key. This information is provided to the ID Confirmation Entity, which is responsible for creating and approving the returned template. User template requests and returned results (Information Flow H) are described as follows:

User Template Request: {user IP#, template ID, template name, template location, Required Template Information [name, address, affiliations etc], Identity Confirmation ([IdB #, IdB location (IP #) (Identity Broker)] or [Account #, Account Password (Encrypted) (Existing Relationship)])}

Returned User Information Template: {template ID, user ID, template #, [information template (digitally signed by ISP)]}

Users can also request information on a template that is in use within surrounding intelligent environments. Template information requests are made by sending the Template Name and ID (to view where a template is used) or the Intelligent Environment Name or ID (for a list of currently used templates in an intelligent environment). The required information is then gathered from the Services or Templates Database. This exchange (also labelled as Information Flow H) is in the form of:
Information Request: {request type (0 or 1), request details ([template ID, template name, template location] or [intelligent environment name, intelligent environment location (IP#)])}

Information Returned: {template ID, [intelligent environment name, intelligent environment location (IP#)], service title, service location (IP#)} OR: {intelligent environment name, intelligent environment location (IP#), [template ID, template name, service title, service location (IP#)]}

Intelligent Environment Services are able to access generic descriptions of the contents of the information templates to improve how they access information provided in these templates. By being able to verify a template ID and issuing location, an intelligent environment’s service providers are able to make a determination on the trustworthiness of the template’s issuer, and thus the trustworthiness of the signed template’s information. This ability to determination a template’s trustworthiness is essential for the effective use of this information authorisation entity. Template requests and responses (Information Flow F) to the Service Providers are of the form:

Service Template Request: {template details [template ID, template location (IP#), Service Title, Service Description, Service Location (IE Name), Service Location Address (IP#)]}

User Template Information: {template ID, template location, [template information description]}

6.2.6.2 Templates Database

The Templates database stores information on all templates created by the ISP, including generic template information descriptions (used by Service Providers to improving parsing of these templates) and records of each template issued to a user. The Template record element describing the generic template types includes the template’s name, location, issuer, a generic information description (for parsing assistance) and policies governing the template’s creation and any specific identity requirements (e.g. must be a university student). The User Templates record element describes the user and template IDs, the signed template and a brief description of the confirmation entity used to verify the user’s information (for example an Identity Broker’s address). This information is described in Figure 20.

<table>
<thead>
<tr>
<th>Template</th>
<th>User Templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template ID*</td>
<td>Template #*</td>
</tr>
<tr>
<td>Template Name</td>
<td>Template ID</td>
</tr>
<tr>
<td>Template Location (IP#)</td>
<td>User ID</td>
</tr>
<tr>
<td>Template Information</td>
<td>Signed User Template</td>
</tr>
<tr>
<td>Description</td>
<td>Confirmation Entity (IdB Address / Internal Account Number)</td>
</tr>
<tr>
<td>Template Issuer</td>
<td></td>
</tr>
<tr>
<td>Access Policy (Creation Rights)</td>
<td></td>
</tr>
<tr>
<td>Identity Req. (Specific ID Req.)</td>
<td></td>
</tr>
</tbody>
</table>

Figure 20: Template Database

The Template record element provides structural and issuing information on a template issued by an ISP. The template has basic description information (Template ID, Name and Description), issuing information (minimum Identity Requirements, Access Policy and the Issuer Name) and the location of the template schema that services can use to automatically read user information.
6.2.6.3 Identity Confirmation Entity

The Identity Confirmation Entity is responsible for authenticating the identity assertions provided by the user to be signed by the Information Service Provider as true and correct. This could be accomplished by contacting a third party (e.g. an Identity Broker), or by accessing the user’s information from an existing relationship (i.e. a user’s employer or university might provide these types of templates). The Identity Confirmation Entity is different from the Identity Confirmation Authority in the Identity Broker (see section 6.2.7.3) as the this entity relies on a third party to authenticate an identity assertion.

The information relationship used to confirm the user’s identity is provided by the template request (see section 6.2.6.1). The ID confirmation entity uses this information to access either the internal user account or to request the confirmation of the template information from the external Identity Broker. This confirmation uses the same process that is described in section 6.2.7.

6.2.6.4 Services Database

The Services database contains information on the templates in use within intelligent environment services worldwide. This information could be used to inform users of the information templates that they could easily use within a given intelligent environment, or conversely to investigate which intelligent environments currently use a particular template. The database contains a description of each template, summaries of usage and a description of where each template has been used. The Services database is modelled in Figure 21, while its access is described in section 6.2.6.1.

<table>
<thead>
<tr>
<th>Template</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template ID*</td>
<td>Service ID*</td>
</tr>
<tr>
<td>Template Name</td>
<td>Service Title</td>
</tr>
<tr>
<td>Template Location (IP#)</td>
<td>Service Description</td>
</tr>
<tr>
<td>Template Information Description</td>
<td>Service Location (IE Name)</td>
</tr>
<tr>
<td>Template Service Summary</td>
<td>Service Location Address (IP#)</td>
</tr>
</tbody>
</table>

Figure 21: Services Database

6.2.6.5 Privacy Threats and Analysis

Information Service Providers’ signed digital templates contain information that users want to share with services and other third parties. This means that users’ privacy is unlikely to be affected by their disclosure. One possible concern, however, is the use of multiple templates with variations of the same information that might be used to link the user’s interactions between visits. The service interaction interface that users utilise should allow users to see what information they have applied to this particular service provider in the past. This should help users determine the privacy risks of a particular interaction. These risks can be further mitigated by not having unique or personal identity information within the templates wherever possible.

ISP templates will often have limited life spans, as the trust determinations made by the intelligent environment’s services could change over time as perceptions of the issuing organisation change. Older templates might also be
rejected, especially if the information represented is likely to be transient in nature (e.g. that the owner is a university student). A method of remotely updating and managing users’ digital templates should be included in their interaction interface.

The last privacy threat to the user from using these digital templates is the chance that the integrity of the Information Service Provider might be compromised, and the user’s information might, through hacking, social engineering or poor business practices, be exposed to malicious third parties. This threat is difficult for the user to mitigate, but could be avoided by employing trustworthy organisations that have experience in maintaining the security of users’ records. A government department or major banking institution would be the logical choice to provide these services, as would other organisations with a good reputation (e.g. a university).

### 6.2.7 Identity Broker

An Identity Broker (IdB) is a third-party entity that maintains users’ accounts that can be used to confirm all or part of a user’s identity. These entities provide identity authentication of facts asserted by the user for service provision, and could be used to confirm and process payment of a service. These entities provide strong authentication of an identity or persona, and are similar to the identity providers described in the Shibboleth, U-Prove and Liberty Alliance frameworks.

The identity broker would normally confirm only specific parts of a user’s identity, for example that they are over 18, providing just enough information to confirm the request. A user would most likely have multiple identity brokers, each for a specific facet of the user’s identity, such as financial data, user details, medical information etc. To improve anonymity and reduce the potential for inference attacks, or the creation of an imposed persona with all of the user’s personal information, one user identity account should have multiple references for each account. Users should also maintain multiple accounts with different brokers.

The identity broker has been implemented in Python as a simple database, checking whether a particular user’s detail (name, age, etc.) is within the user database. The information request is sent to the identity broker (see Information Flow J), and the broker confirms (returns ‘1’) or rejects the request (returns ‘0’). The identity broker allows multiple account numbers to refer to the same account, to improve location-based anonymity, which will vary by design with what information can be accessed from the database (for example, a basic identity database might only allow the confirmation of identity, while a medical database may provide all medical information that is requested).

#### 6.2.7.1 Broker Connection

This entity accepts requests for identity confirmation from third parties and manages the secure communication of the results back to the requesting entity. All requests for confirmation of identity (see Information Flow J) are passed to the ID Confirmation Authority, which then returns the request’s
results after consulting the Broker’s Identities Database. The information requests are shown below:

Identity Confirmation Request (to IdB location (IP#); encrypted: IdB Pub Key): {IdB #, request type (send=0, confirm=1), [information to confirm], service location (IP#), servers Pub Key}

Identity Confirmation Response (to service location (IP#); encrypted: Service’s Pub Key): {Confirmation (True=1, False=0), [requested information]}

Communication with the Identity Broker is encrypted using a single session key provided by the intelligent environment’s Kerberos Server when available, and using the Identity Broker’s public key when it is not. In the latter case, information, encrypted with the service provider’s public key, is sent back to the intelligent environment’s service provider.

6.2.7.2 Broker IDs Database

This database contains all information associated with a particular identity account. This information could contain health, financial or personal information or indeed any information that the user wants to be able to confirm privately with a third party. This database is used to confirm or refute any given information about the account’s owner.

Each IdB Account is set up by the user to serve a particular purpose, such as confirming financial or health records. These accounts are referenced by their IdB Account ID, which is passed to the Identity Broker complete with a local time stamp. This exchange of information encrypted by the IdB’s Public Key should contain the user’s Identity Broker Account, and a Hash of their password. The time stamp is useful for preventing further tests of the user’s information, and only requests stamped with a sufficiently recent time will be accessed. The user’s Identity Broker should also record all verification requests to enable the user to review how his identity account is being queried and for repudiation in case of malicious use of his identity account. The information contained within the Broker IDs Database is described in Figure 22.

<table>
<thead>
<tr>
<th>IdB Accounts</th>
<th>Interaction Histories</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdB Account ID*</td>
<td>IDb Account ID</td>
</tr>
<tr>
<td>Password</td>
<td>Request ID*</td>
</tr>
<tr>
<td>First Name</td>
<td>Request Type</td>
</tr>
<tr>
<td>Last Name</td>
<td>Information Requested</td>
</tr>
<tr>
<td>Age/Date of Birth</td>
<td>Requestor Name or ID</td>
</tr>
<tr>
<td>Public Domain</td>
<td>Return IP Address of Request</td>
</tr>
<tr>
<td>Account Holder Information</td>
<td>Request Result</td>
</tr>
<tr>
<td>- Financial Records</td>
<td></td>
</tr>
<tr>
<td>- Biometric Information (e.g. Fingerprints)</td>
<td></td>
</tr>
<tr>
<td>- Personal Description/Details</td>
<td></td>
</tr>
<tr>
<td>- Medical Records</td>
<td></td>
</tr>
</tbody>
</table>

![Figure 22: Broker IDs Database](image)

6.2.7.3 Identity Confirmation Authority

This entity accepts identity information requests (from the Broker Connection) and authenticates the identity assertions by querying the 'Broker IDs
Database’. It then returns the result to the Broker Connection, which passes the result back to the requesting entity. The Identity Confirmation Authority is different from the Identity Confirmation Entity (see section 6.2.6.3) in the ISP as the Authority has the identity information database and does not use a third party to authenticate an identity assertion.

A potential weakness of the identity broker is that it could conceivably be used to trawl for information about the user (an ‘Inference Attack’), with multiple information requests slowly building up a profile of the user. This is avoided by the inclusion of current time and date of the user’s mobile device with their Identity Broker account when making a service request. This means that the intelligent environment is able to reject the reuse of any information requests by rejecting any time and date stamp already used. Further security could be realised by using account numbers only good for one usage, but this is unnecessary with the time and date information included in the encrypted account packet.

### 6.2.7.4 Privacy Threats and Analysis

The use of an Identity Broker represents very little in the way of threats to a user’s privacy. All communication with the broker is encrypted, either using Kerberos or directly using public keys. The user’s identity broker account number is never disclosed to the intelligent environment’s service provider, and is encrypted along with the current date and time. This prevents the encrypted account packets from being comparable between sessions and ensures that a service request cannot be reused to mine more information about the user.

The only potential concern for using an identity broker is that, instead of using the request to confirm information already received, the intelligent environment will use the access to request other information (e.g. obtaining the user’s name instead of confirming their age). This could be avoided by adding an ‘allowable requests’ checksum in the user’s encrypted IdB account number packet stating which request can be served (i.e. ‘1’ for confirm only, and ‘0’ for any). The other option would be to disable this feature, but there are likely many reasons why this would not be desirable. For example, limited battery power and encryption capabilities might make it unfeasible to transmit this information wirelessly from the user’s mobile device.

The last privacy threat to the user from using an Identity Broker is the chance that the integrity of the Identity Broker might be compromised, and the user’s information might, through hacking, social engineering or poor business practices, be exposed to malicious third parties. This threat is difficult for the user to mitigate, but could be avoided by employing trustworthy organisations that have experience in maintaining the security of user’s records. A government department or major banking institution would perhaps be the logical choice to provide these services, but numerous serious breaches of public data continue to reduce people’s confidence in these institutions’ ability to maintain the privacy of their customers or citizens.
6.3 Prototyping of SPACE Compliant Infrastructure

An implementation of the SPACE architecture was developed in Python (version 2.5), based upon the architecture’s design described in Figure 12. The implementation allows users to logon to a user register, investigate and interact with services provided by the environment, exchange information with other users (and their personal domain) and selectively manage users’ personal information exposure when interacting with an intelligent environment. The implementation was iteratively developed since the development of our initial architecture, shown in section 4.4, to integrate the required infrastructure components and to address users’ privacy and security concerns. The relationship of this research activity to others within this dissertation is described in Figure 6.

Interaction between users within this implementation is text-based, but users are able to request more information from another user’s personal domain. The concept of different personae for different interaction tasks was communicated by the information provided back to the user based upon the persona they are logged in with. Whilst the system was not tested over a wireless network, it was successful in providing a test bed for the final SPACE architecture (described in Figure 13). This implementation was useful in demonstrating the technical realities of interacting with an intelligent environment, and it allowed a thorough investigation of communication within the environment and with its identity management structures.

6.3.1 Design Discussion

This implementation was essential for the evaluation of the technical security provided for users interacting within the SPACE architecture. It provided a method of tracking users’ information throughout their interaction with the environment, its services and other users. The implementation also provided the authors with a clearer understanding of privacy risks associated with exchanging information within an intelligent environment. This knowledge, along with the technical realities of communicating within a ubiquitous computing environment, led to the improvement of the SPACE architecture and to the design described in Figure 13.

This development of the SPACE architecture was limited by the available resources. To reduce development time, and to increase the resources available for the user studies and analysis of the architecture, parts of the SPACE architecture were simulated. These simulations were made where they would have no impact on the core functionality or on the analysis of the SPACE architecture, and where the components have been tested in other implementations or user studies. These components are: the use of a Kerberos server to manage the exchange of encryption keys; the implementation of digitally secured pseudonyms (normally provided by the Information Service Providers); external implementation of the Identity Manager, Identity Broker and the user’s Personal Domain; and the use of a graphical user interface to manage the exchange of information within an intelligent environment.
Kerberos servers have been widely implemented in distributed computing environments. This implementation used public key encryption, with static public and private keys, to demonstrate the secure exchange of information within the environment. A fully functional intelligent environment would use both of these systems for information security. The Kerberos server would be the initial and most commonly used encryption method, with the users’ and intelligent environments’ key pairs being used in the absence of a central key distribution server. This method of implementation allowed the use of current PDAs that would otherwise be unable to handle the strong encryption requirements. This problem will be made redundant as more powerful handhelds become available. The SPACE architecture calls for the use of random MAC addresses in our environment. These were previously demonstrated in (Gruteser & Grunwald, 2005), and have not been implemented into this implementation.

The identity structures within the SPACE architecture were implemented on a single machine, simplifying the bandwidth requirements and network access problems that might have arisen from a distributed computing environment, but this has no impact on the architecture as the connection code remains the same. Due to the resource overhead caused by encrypting large data streams, the pickle python module was used to simulate the encryption and blind packet delivery system developed in the Gaia OS (Campbell et al., 2002). This does not affect the validity of our implementation findings as the Gaia OS packet delivery method has already been demonstrated, and the only information available to the intelligent environment is the Identity Manager’s IP address. This information is not enough to endanger the user’s privacy if other precautions are taken, i.e. the use of multiple Identity Managers, as would be the case in a full SPACE architecture implementation.

Digitally secured pseudonyms have previously been implemented by Hitchens Kay and Kummerfeld (2004), and were left out of this implementation. This drastically reduced the complexity of the implementation, at the cost of not demonstrating an already working system within our intelligent environment. Investigation of the use of secure digital personae will have to use a faked digital template to deliver verified information to the intelligent environment’s services. This evaluation is included in our final user study described in the next section. The mechanisms for determining the trustworthiness of a template provider are described in section 2.4.5.1, but measuring their effectiveness is outside the scope of this research.

The final aspect of this implementation that should be mentioned is the lack of an effective GUI for users to manage the exchange of their information within the intelligent environment. An effective interface should be able to show all previous interactions the current user has had with an environment, and their current and available personae to use for interaction. The interface

---

5 The pickle module implements a fundamental but powerful algorithm for serialising and de-serialising a Python object structure (http://docs.python.org/library/pickle.html).
must also help the user manage multiple interactions with multiple intelligent environments at once.

Existing interfaces have examined the problems of identity management (Jendricke, Kreutzer & Zugenmaier, 2002) and sharing information with groups and services while taking into account privacy legislation and other factors (Price, Adam & Nuseibeh, 2005). More research into the effectiveness of different interface designs is required. Our implementation interface is text-based, and thus would have a difficult time providing its users with adequate feedback on the exchange of information with the environment. Our user study would, therefore, require a more effective user interface, and some aspects of our interaction may have to be simplified.

6.3.2 Findings and Analysis

The iterative development process was imperative in helping the author to understand the requirements of communication between the intelligent environment and its users. Communication between environmental entities, in particular between the user's mobile device and the user register and other services, was easier to model during the development process. The initial architecture highlighted the danger of allowing the user’s mobile device to be recognised and linkable to all previous interactions, which led to preventing the user's unique ID from being available to the intelligent environment. Concern over wireless traffic analysis further led to the development of the Personal Domain to allow information requests to be handled without requiring direct communication with the user's handheld device. This allows us to consider a future with simpler personal devices, as more processing could be done by the user's personal domain.

The purpose and scope of the environment's identity management structures were also easier to define after the development, and this highlighted the types of connections required to access local and global services. The need for greater user pseudo-anonymity, reflected in our user studies (from chapter four), and the possibility of intelligent environments being cut off from the Internet, suggested that a different type of identity management was required, and led to the inclusion of the Information Service Providers in the final architecture to provide secure digital templates and augment the verifiable and user-controlled solutions already available.

The development process made threats to user communications clearer and led to the inclusion of many additional security features, for example, the salting of identity authentication requests with the current time and date to prevent masquerading attacks. Additional security was also added by including a Kerberos server to manage key exchanges for users interacting with the intelligent environment, providing an additional layer of security above and beyond that which was achieved through selective information sharing, point-to-point encryption and through the environment’s identity management and anonymous interaction structures.
6.4 Intelligent Environment Design Requirements

This section examines the evaluations required of the SPACE architecture to ensure that it meets the expectations and design requirements of the ubiquitous computing infrastructure described in chapter five. Of particular concern are the information flow, identity management and personal domain requirements for our architecture described in section 5.3. This section identifies the required architectural evaluations, examines the technical implementation of our architecture that was developed to allow these tests and revisits the user studies that investigated these requirements. The user study described in this section also attempts to verify design decisions made in our initial architecture and those subsequently suggested by user studies in chapter four.

6.4.1 Required Ubiquitous Computing Infrastructure Evaluations

This section examines the necessary evaluations required to ensure our ubiquitous computing infrastructure meets the goals set out in chapter five. These goals include:

- the integration of ubiquitous computing tools to create and interact with digital communities and maintain users’ social networks in real-world environments;
- the delivery of personalised services interaction, whilst providing users with control over their identity and distribution of their personal information; and
- the security to ensure users’ confidence in the ability of the network to provide a secure transport medium for service and community interaction.

The services that could be provided from our ubiquitous computing infrastructure are incredibly varied. ‘Third places’ are community spaces that help promote the casual social interaction that supports community members personally, socially and economically. Ubiquitous computing technologies have the ability to deliver these ‘third places’, by overcoming the lack of presence, accessibility and social levelling that is normally associated with more traditional digital communities. Additional communication and user-centric interaction services allow users to integrate more effectively with their close friend and family networks, whilst maintaining local anonymity.

The SPACE architecture promotes user control over their personal information and identities, and affords users the same interactions in the digital world that they would enjoy in the physical world. For example, users can interact anonymously to maintain their privacy, pseudo-anonymously to gain a more personalised service, or in some cases users will have to prove their identity. These interaction options, and the user’s privacy, are provided by the three different types of identity management in use within the environment. User privacy within our architecture is initially ensured by the anonymous interaction options and the additional safeguards that restrict the movement of the user’s information, but is still vulnerable to poor security in the information exchanges between the user and the environment. The following
sections, therefore, examine identity management and information security within the SPACE architecture, describe how these structures meet the infrastructure goals identified in chapter five, and consider any further examinations that are required by the evaluation user study (in section 6.4.2).

6.4.1.1 Identity Management
The identity management structures integrated into the SPACE architecture allow users to interact anonymously with their intelligent environment until they wish to share specific information in order to receive a service or perceived benefit. Evaluation of the security provided by these services underlines users’ control over their identity within the ubiquitous computing infrastructure. Users choose when and what information they wish to share with the environment, and by what means they wish to share it. Creative use of all three identity authentication mechanisms can provide the user with the desired interaction without exposing any additional information, in a manner that prevents users from being tracked between interaction sessions.

To evaluate the use of our identity structures, the user must be able to understand and effectively use their Identity Manager, Identity Broker and Information Service Provider’s digitally secured templates. Therefore the scenario must make users aware of their identity managers, and allow them access to their configuration and use for private and secure confirmation and distribution of identity. The concepts of identity management are familiar to most users, and their use of minimum levels of privacy to allow interaction with an intelligent environment’s services with limited personal information seeks to reduce user anxiety about interacting with an effectively invisible environment. Users’ reaction to the use of identity brokers should therefore be addressed in our final user study.

The first test measures users’ perceptions of the use of an external Identity Manager and the use of centralised identity storage (or the use of the Identity Broker). Users are first asked to configure their privacy preferences, and then are given the opportunity to interact with other users’ Identity Manager. This test examines user perceptions about the management of identity in this fashion, and the implementation is used to allow the identity management framework for this architecture to be investigated. Users are asked a number of follow-up questions investigating the strengths and weaknesses of this approach.

The use of Information Service Providers is investigated to determine users’ perceptions of an external third party providing infrastructure for intelligent environments. This test examines users’ perceptions of this external entity, and provides a chance for the investigation of its use in intelligent environments. Users are asked a number of questions regarding the usefulness of this entity, and to identity any services that could be utilised in this manner. The user scenario for this evaluation must allow users to access and use the external Information Service Provider, and allow the users to see the benefits of using this service. Our final user study presents the use of secure digital templates to access a campus food delivery service.
6.4.1.2 Information Security

The effectiveness of the security within the SPACE architecture will determine how much trust users can place in the privacy mechanisms and guarantees that are designed to promote user’s usage of this ubiquitous computing environment. The SPACE architecture follows the concept of multilateral security in restricting access to information by the information’s owners. Service information is controlled by the service delivery entities, whilst users have control of their information on their personal domains and mobile devices, and have control of which information they exchange in order to receive something of perceived value (the service).

Intelligent environments can use the benefits of their geographical positioning to address common problems in system availability. Through the use of local services, the SPACE architecture requires users to be physically present in the local environment (instead of allowing remote service access). Any denial of service attack must therefore be made from within the local environment. Global services could face denial of service attacks, so these services require the denial of service protections already developed for Internet websites. Decentralising the access points for global services would further reduce their vulnerability.

The use of a random unique identifier in the SPACE architecture (from the user’s mobile device) might make it easier for those engaged in the attack to avoid detection, but a sustained attack on available system resources would be unlikely given the proximity requirement. Services that are particularly susceptible to denial of service attacks may further require access authentication from the user register, through the exchange of a session key to allow encrypted communication with the service entity. This would not cause legitimate users any difficulties, as they could still log in anonymously. This would make the denial of service approach less feasible due to the number of physical machines that would be required in the environment.

The SPACE architecture requires the use of a session management system whenever any privacy or information security is required (for all but the most open, anonymous interaction system). A Kerberos server running on the user register provides any session keys required to provide secure communication within an intelligent environment. When this is not available, the service providers and user registers provide public keys that can be used to send their information and service requests securely. Due to the already proven ability of the Kerberos server to integrate with ubiquitous computing environments (for example see the Gaia OS (Campbell et al., 2002)), integration with the SPACE architecture was not carried out to reduce the required implementation effort.

The initial intelligent environment prototype was implemented using an existing public key encryption module. This was used to encrypt the identity account numbers (for the Identity Manager and the Identity Broker) to protect their contents during transmission. This implementation demonstrated that any malicious third party intercepting the transmissions could use this information to compare with previously sent data, and in doing so might be
able to match the encrypted identity account to one that was previously supplied.

The sending of identity numbers without encrypting them could expose the users by allowing their interaction histories to be matched between sessions. This might also be done if the identity numbers are encrypted with the same public key each session, leaving the user vulnerable to a ‘reply attack’. This could lead to the creation of a detailed user profile to be applied to the user against their privacy wishes. The SPACE architecture requires identity account numbers to be encrypted with a date and time stamp, or salted, to avoid reuse and to prevent them being recognised between interaction sessions. The encryption of identity account information is necessary as it will be provided to a (potentially untrustworthy) intelligent environment as part of the user’s logging in to the user’s register, or as part of a service usage request. To prevent the destination address to be used in a similar way (to match user’s interaction sessions) the destination is either a blind relay (that would change with use) or an entity with a large number of identity accounts (e.g. an Identity Broker).

The authentication of users interacting with the service entities requires some form of identity management, including the Identity Broker, Identity Manager and the secure digital templates provided by Information Service Providers. The physical accessibility of intelligent environments, however, causes some concerns about the intelligent environments’ vulnerability. Intelligent environments could potentially be tampered with (either physically or digitally) either to collect user information for profit or to provide a fake intelligent environment service for malicious reasons. The use of trusted computing components allows users to verify the intelligent environment’s identity (and compare discovered services to previously encountered environmental services). Local directories describing available intelligent environments, and their services, should be compiled and made available to users.

The secure storage of information within an intelligent environment has been discussed previously in section 5.2.5. Trusted computing components are used by the user and the intelligent environment to encrypt their user and service usage information on the environment’s hard drive. Interaction summaries are maintained separately by the intelligent environment. This prevents the unauthorised access of users’ information when they are not interacting with the environment, but allows interaction summaries and other useful information to be available to the environment’s owners to allow them to improve their service delivery.

### 6.4.2 Evaluation User Study

The final user evaluation of the SPACE architecture was conducted as a field study within a university environment, using simulated context-aware services. This study incorporates some of the benefits of a laboratory experiment, namely the ability to control the reaction of particular services to users’ interactions whilst maintaining the field experiment’s localisation of the phenomenon under study within its natural environment. The localisation of
Chapter Six: A Solution for Privacy in Ubiquitous Computing

the study of a familiar environment will provide the participants with greater context and meaning, which should also improve the realism of the available services. The services provided by the intelligent environment are appropriate for their given context, and the users may have used these services in the past on a different platform (e.g. using the school webpage).

6.4.2.1 User Study Description

The user study was conducted to investigate users’ reactions to the interaction provided by the developed intelligent environment architecture (see Figure 12). Participants were invited to interact with two intelligent environments that provide environmentally-specific services and access to local information. The intelligent environments covered a common use computing facility and the greater university campus area. The intelligent environments were developed using mod_python and were accessible via a web browser on handheld or traditional computing devices. Participants were solicited from throughout the university by advertising within the science and information technology schools.

The user study uses two iPaq PDAs to connect to a central server via a wireless Internet connection. It uses mod_python to interface with the environment and dynamically generated HTML sheets to simulate the service interface personalised to the user’s interaction preferences. These preferences described the type of identity information (or personae) the user can share with the environment, and the services made available to the user depended upon the persona selected. The personae available were: completely anonymous; a persona that identified the user as a university student (but not the user’s name); and a final persona that identified the user by name that provided access to university services.

The user study (N=18) consisted of exploring the two intelligent environments’ services and answering questions on the experience and possible use of services. Volunteers for this study were recruited on the basis that they would likely be early adopters of technology, so we sought out accessible, young people familiar with information technology. This was reflected in our survey population most of whom were students, under the age of 30 (72%), identified themselves as being in the IT field (83%) and owned a mobile phone or PDA (89%). No financial compensation was provided to the eleven men and seven women who took part in the study.

6.4.2.2 User Study Results

The study began with a briefing on the nature of the intelligent environments and user pseudonyms, and a brief introduction to the Intelligent Environment Interface (see Figure 23). Users then logged into each environment and investigated the available services. Three pseudonyms were available to the user: Anonymous, University Certified and Identifiable pseudonyms demonstrated the escalating levels of access to services. The University Certified pseudonym allowed the environment to identify that the user was enrolled, and therefore entitled to access university services, but did not provide any personal information. When the users were familiar with the
environments, they were questioned on their interaction with the environments’ services.

![Intelligent Environment Interface](image)

**Intelligent Environment Interface**

- **Location:** M44 - Building foyer [view]
- **User Name:**

**Devices**

- Air Conditioning: air conditioning controls. [link]
- Common Access Printer: locate nearest accessible printer. [location]
- Postgraduate Printer: Locate nearest accessible Postgraduate Printer. [location]
- Security: Security services, microphones, and video cameras capture information for the room’s smart lighting sensors for energy conservation. [info]
- School of ICT Information Centre: Access the school’s subject database. [subject] [homepage]

**Locations**

- Postgraduate Workspace: Location of ICT Postgraduate Workspace [location]
- Campus Map: University campus map. [location]
- Science Common Room: Directions to science common room. [location]
- Toilets: Directions to the Toilets. [location]

**Services**

- Wireless Networking [Wireless]

Reconnect to User Register

Returns to Intelligent Environment Main Menu

**Figure 23: User Study Intelligent Environment Interface**

All users indicated that the intelligent environments provided valuable services. Primarily users liked the direct and easy access to local information (e.g. Maps, directions etc.) and the ability to control what information the environment knew about the user. Users also enjoyed the collection of links to useful, external services. This highlights the strength of this architecture, allowing users to interact not only with locally hosted services, but also with useful Internet-based information services (e.g. News, Weather, Internet Search Engines etc.).

Users were asked at this point in the study what improvements they would like to see in the interface or in the interaction with the intelligent environment. Thirteen participants responded, with seven users calling for better navigation options (including the use of graphics in the user interface), two users suggesting new services and two users asking for the system to be ported to a mobile phone platform. One user required more feedback on the exact information being exchanged, and the final responder suggested the minimalist interface was ideal for the services being delivered.

To further illustrate the use of user pseudonyms in this environment, users were shown a more advanced interface that contained more information on each pseudonym (Figure 24). These interfaces clearly show the information associated with each pseudonym, and showed the type of interaction and feedback possible. Upon reflection of the new and original intelligent environment interfaces, all users agreed that this use of user pseudonyms would be an effective method of controlling which information the intelligent environment has access to.
When asked to comment on why the new pseudonyms were an effective means to manage information exchanges with the environment, sixteen people responded. Twelve users replied with variations on stating that this interface allowed the user to provide only the information that is required to the environment. One of these comments sums this up thus: "I can vary my exposure as I desire, to get what I want. ALSO I can see the relevance of the required information." This user also stated that he was very happy with this interface as it fitted his mental model of what was required. Another respondent stated the interface "Allows you to be anonymous, and to manage your exposure." One of these respondents questioned the security in use for storing the payment information on the shopping pseudonyms, highlighting that any interface must be prepared to justify the security in use to its users.

Two users responded that the interface would improve service delivery, as the interface could provide instant (and personalised) access to a service. Another comment noted that the interface used the same type of access control actually used on the university services. The final response highlighted how easy to use the interface appeared to be. This interaction method describes the use of user-selected pseudonyms, described in section 6.5.2.

Users were then asked to describe "What type of feedback you would like to receive when interacting with an intelligent environment?". Responses (see Table 16) indicated users were most interested in 'How collected information will be used' (89%) and ‘What information is collected by the intelligent environment’ (72%). The relatively high percentage of responses suggests users are suspicious of data-collection activities in these environments, and want as much information as possible when evaluating the privacy risks versus the rewards of using a service. Other responses to this question included requests for an environment’s contact information, to allow reporting of misuse or system errors, feedback on the level of governmental control over the intelligent environment and mandatory date stamps on environmental information to allow users to determine its validity.
What type of feedback would you like to receive when interacting with an intelligent environment?  

<table>
<thead>
<tr>
<th>Feedback Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>How collected information will be used</td>
<td>88.9%</td>
</tr>
<tr>
<td>What information is collected by the intelligent environment</td>
<td>72.2%</td>
</tr>
<tr>
<td>Previous interactions you’ve had with this environment (or service)</td>
<td>61.1%</td>
</tr>
<tr>
<td>How long collected information will be stored before being deleted</td>
<td>55.6%</td>
</tr>
<tr>
<td>A third party evaluation of the intelligent environment’s reputation</td>
<td>55.6%</td>
</tr>
<tr>
<td>Feedback on how to better interact with the environment (or service)</td>
<td>55.6%</td>
</tr>
<tr>
<td>Information on the owners and managers of the intelligent environment</td>
<td>44.4%</td>
</tr>
</tbody>
</table>

Table 16: Desired Intelligent Environment Interface Feedback

Users were asked to first identify the most useful services offered by this intelligent environment, and what other services they would be interested in seeing. The most popular services were location finding or direction services (13 users, 72%), access to local information (7 users, 39%), and access to local public transport timetabling information (7 users, 39%). Further suggested services focused on the delivery of specific environmental information (e.g. parking information) (5 users, 28%) and access to contextual information on the environment (e.g. computer available in a common use lab, current traffic levels, etc.) (5 users, 28%).

The final stage of this user study involved users interacting with a service using a ‘Secure User Template’ issued by the Information Service Provider. In this task, users accessed a simple food delivery service, and were able to call up their information using a ‘Load User Template’ button. This interface can be seen in Figure 25. Users were then asked, post interaction, whether they would consider this an effective method of providing their information, and what types of services they would like to use this with. After using the interface, all users agreed that it was an effective method of interaction, although some users raised concerns on how the information was stored and secured. When this type of service is integrated into a service interface, the user must have access to what information is stored, and a description of how it is secured.
Figure 25: Example Service using ‘Secure User Template’

To finish the evaluation, users were asked, if their information could be maintained and used privately and securely, what information and services they would like to interact with. Those mentioned were services that provided location and map-based information, integration with local shops (many kinds), banking and e-commerce, delivery of products, food ordering, public transport information and local environmental information. Users were wary of storing confidential information (like medical records), and suggested they would only start ordering from stores (e.g. coffee) once the technology had matured.

Users were then asked more generally about the types of functionality they would like to see. Users expressed their support for improved access to community information and the Internet, and the ability to communicate (and selectively share their location) with friends and family. However, this was tempered by the usual privacy and security concerns regarding the use of ubiquitous computing technologies and the sharing of users’ personal information (particularly financial information or children’s personal details). These results indicate that methods of securing users’ information and maintaining the environment’s security must be as transparent as possible to promote users’ confidence in this new method of information delivery.

6.4.2.3 Design Implications

The use of user pseudonyms to control the exposure of users’ personal information when interacting with intelligent environment services has been suggested in other research. This user study had to develop users’ understanding of pseudonymous interaction in order to allow them to consider what types of information could be used, and how this would affect their interaction capabilities. The participants had no trouble accepting this interaction technique, and users’ responses suggest that they were much
more likely to interact with the environment’s services if given the opportunity to manage their identity exposure and receive appropriate feedback on information collection activities. The SPACE architecture provides this interaction with the Persona Manager that manages the persona selection and identity management requirements for both the Service Manager and the User Manager.

The user’s interaction interface is essential in helping determine the risks of service interaction to their privacy. The overwhelming percentage of users wanting feedback on what information was being used by the system, and how it was being used, shows that users are concerned about information collection. These results are not surprising considering the strong concern users have shown for “Big Brother” type information collection systems, but, given the support for the services provided by the intelligent environment, it is possible that users will begin acting against their privacy preferences (see section 2.4.2.3).

Other feedback that users have requested includes previous interaction with the environment, the environment’s owners and information storage policies, external feedback on the environment’s reputation (see section 6.5.3) and help from their mobile device in improving their interactions with the intelligent environment. These results are supported by our earlier user study results (especially in sections 4.2 and 4.5), and show the distrust in invisible information collection common to all ubiquitous computing user studies. A method of ensuring that the advertised information collection and reuse policies were followed would be a positive step towards alleviating these fears. This is investigated in section 6.5.1.

The investigation of the environment’s services reinforces the external validity of this field experiment. All the services were identified as useful by the participants, and they observed that the services presented are what they would expect the environment to provide. This view of the environment underscored that users felt this was a natural interaction environment that matched the anticipated reality of intelligent environments. The controlled nature of the experiment, however, allowed the users to focus on service interaction and their perceptions on the impact of using these services upon their privacy. This focus should improve the internal validity of this field study.

The services highlighted as most useful by users were local information, location or direction services (i.e. environmental services), and access to central databases for more global information (i.e. global services such as our public transport timetable database). In addition to additional environmental information requests, much user enthusiasm was shown for contextually relevant services that highlighted an important but likely transient aspect of the environment (e.g. the current state of computer rooms, Internet traffic and car park usage). Results of this user study further underline the need for services that support community interaction (described in section 5.2).

The participants were attracted by many different services within our environments, but were mostly drawn to the easy to use services that could provide contextually relevant information. The potential usefulness of the
suggested global and environmental services, along with the ability to integrate existing Internet-based applications (like location-aware public transport timetables) into our intelligent environments, is compelling. The increasingly pervasive reach of wide-area wireless Internet access continues to suggest that these environments will be technically easy to implement in the near-to-medium term. Intelligent environments that do not provide Internet access would seemingly be arbitrarily reducing their value. Our experience and research reviews suggest that environments that do this are more likely to be the exception, based upon a specific security concern, rather than the rule.

Feedback from users over our identity management structures indicates that users need little to no instruction to grasp the basics of our identity management schema, which is the graduated pseudonyms or personae that users can adopt to achieve different levels of anonymity. The study found support for using user templates for personal information delivery, but, as with most new identity management structures, the users are suspicious of yet undiscovered technical flaws that could be exposed to malicious third parties. Users need to be educated about the security employed within each method to ensure that they are safe. The adoption of these identity structures will improve as more people use them and as more experts and public figures declare they are safe.

6.4.3 Summary and Conclusions

This section evaluated the technical security and logical privacy design of the SPACE architecture. User privacy within the SPACE architecture is provided by the anonymous technical interaction mechanisms users utilise when interacting with intelligent environments and the control the user has over the exchange of their personal information. All user information is provided in accordance with the user’s privacy preferences from their mobile device, either automatically or when directly authorised by the user. All information exchanges are encrypted, and the personal information that can be used to identify the user between multiple interactions with the environment is also encrypted (e.g. Identity Broker or Identity Manager Account numbers).

An implementation of the SPACE architecture was developed to provide an interaction test bed for the user study, and to allow an investigation into the security of any exchanged information. Some aspects of the SPACE architecture implementation were abstracted when this did not affect our ability to investigate the necessary privacy and security protections in place. This was particularly true for technologies or concepts that have been studied or implemented extensively in similar or equivalent settings (for example the Kerberos key server). This implementation highlights the need for trusted computing components, external Internet access and the need for redundant security features to avoid unintended collection of user information by the environment or its inhabitants.

Users within the SPACE architecture can be vulnerable when interacting with the User Register or when using the environment’s services. Providing identifiable personal information to the User Register may allow the
environment or other users to recognise the user between visits, potentially damaging the user’s privacy. To avoid this, we could eliminate all user interaction that uses this personal information, but this removes the casual community interaction that our architecture is meant to support. A better solution is to educate users on the risks of these interactions, as this still allows new interaction methods to evolve between community members. Service providers should allow anonymous user interaction wherever possible. This includes the use of digitally signed templates, but could include allowing using basic user name and password sign-ons to allow personalised interaction within requiring the user’s identity. The effective management and provision of anonymous environment and service interaction is critical to the success and acceptance of our intelligent environments.

6.5 SPACE Architecture Extensions

This section describes three extensions to the SPACE architecture that improve either information security or user privacy. Two of the extensions have already been implemented in different intelligent environments, and User Selected Pseudonyms extends the intelligent environment interface and provides a new interaction mechanism to improve user privacy. These extensions:

• provide additional security for information stored within an intelligent environment;
• provide an interaction method that users could use to improve anonymity in service interactions; and
• provide more feedback information to allow users to determined risks of information exchanges to their privacy.

These extensions have not been implemented into the SPACE architecture due to the large amount of development effort and environmental infrastructure that would be required, and due to the resource limitations of the dissertation.

6.5.1 Information Tagging

Whilst user privacy primarily comes from the limited use of their information within intelligent environments, our architecture must also consider how we can improve the security of information that is provided to the environment. The SPACE architecture mandates that user information gathered to either personalise or access a service should be encrypted on the intelligent environment’s hard drive used by the user and the environment using their trusted computing components. The multi-tiered storage allows the environment to utilise valuable interaction summary data, whilst protecting the user’s information from reuse. This system protects users by preventing their information from flowing across natural borders of privacy.

Intelligent environments could also use an alternative method of controlling information reuse. A method of tagging information in a manner that would restrict its reuse would allow most sophisticated uses of the data to evolve in accordance with the user’s original privacy preferences, beyond the simplistic
current environment which requires the user be present to unlock their data. Information tags (Jiang & Landay, 2002) have been suggested as a method of controlling information reuse, with (metadata-like) ‘privacy tags’ attached to stored information dictating how this information can be stored, replicated or reused. These ‘privacy tags’ could limit information reuse to particular environments, user groups, networks or even contexts (e.g. only in an emergency).

The privacy tags infrastructure requires that all systems have trusted computing components and that all the systems are trustworthy. This is thus not relevant for the ubiquitous computing infrastructure as a whole, because the infrastructure will likely be made up of mostly untrustworthy systems that provide low security services (e.g. public transport timetables or local directions). But this infrastructure could easily be integrated into subsections of the infrastructure that is trustworthy, like a corporate office network that also provides services to the public. A system’s trustworthiness could also be independently rated by public or private trust and reputation systems (see section 6.5.3).

### 6.5.2 User Selected Pseudonyms

User Selected Pseudonyms (USP) is a method of managing user identity and service interaction across multiple intelligent environments. USP is integrated into the Persona Manager of the SPACE architecture, and its responsibility is to identify the best persona or service account to use when interacting with a particular service. Users requesting access to an environment’s services have three interaction options: provide the environment with a previously used pseudonym (i.e. history of interaction), create a new pseudonym or remain anonymous. Users can maintain many different environmental pseudonyms, allowing them to effectively choose their required level of anonymity at any given time.

Many services, whether or not they require identity authentication, use accounts to record prior interaction with the service and to personalise future interactions. This personalisation can be very useful for interaction with a service, particularly if the service gathers information for the user (e.g. a news service) or if the service has a particularly complex interface. These service pseudonyms could then be copied or edited as the user sees fit to give them multiple interaction options, which users can use to automate information gathering and service usage, such as receiving updates on public transport scheduling and news bulletins while travelling to work, or ordering ‘breakfast to go’ from a favourite café while still on the train. The usability of the USP interface is critical to the success of this pseudonym management solution and to users’ ability to control exposure to their personal information and subsequent dangers to their privacy.

When a user accesses a service for the first time, their handheld computer provides the provider with a random identification number, similar to a user placed ‘cookie’, with which it can store any personal details or user preferences recorded throughout the user’s interaction with the environment. The handheld computer could automate the storage of the ID number, or the
user could annotate the ID reflecting its intended use or privacy exposure, e.g. 'Anonymous News Gathering', 'High Risk', etc. The account linked to the ID number remains within the intelligent environment, and the interaction information within this account can be used to inform the environment’s designers on the usage of the environment. Services that require identity confirmation would still need to secure this information, as described in section 6.2.6.4, to prevent unauthorised reuse of their personal information.

6.5.2.1 Interaction Example

Consider the case of Belinda, a postgraduate student using an interactive bulletin board outside her school’s office. This bulletin board could be used to access local school or university information or provide information accessed from other sources, e.g. bus timetables. As Belinda approaches the board, her mobile device recognises the request for identity information from the board and seeks to supply this information in accordance with her privacy preferences. Belinda’s mobile device selects a pseudonym (or identity account), previously placed in the bulletin board’s database, which contains her desire to see only post-graduate or general university notices.

The bulletin board is able to use the information within the identity account to personalise the displayed information, without breaching Belinda’s privacy by sensing, evaluating or recording personal information. If Belinda had her preferences set differently, then an alternative account may have been provided, possibly containing a list of her subjects so she could receive any notices relevant to her studies. This selection of accounts allows the user to clearly see what information the intelligent environment, in this case the interactive bulletin board, is using to personalise the user’s interaction with the information services. This transparency allows users more control over their privacy and potentially greater confidence when interacting with these environments.

6.5.2.2 System Description

This system replaces the existing methods of service interaction and traditional methods of recognising a user in an intelligent environment, for example, requesting a user name or through the detection of a device’s MAC address. Figure 12 describes the interaction between the user and the intelligent environment. Users interact with an environment with their personal device, which identifies itself to the intelligent environment by providing an existing account stored in the environment. The intelligent environment maintains a model of the environment based upon the information provided by hardware sensors, models of users present in the environment and the available services. Sensor data could include environmental conditions such as the temperature, or the expected arrival of a particular bus at a bus station. Service information describes available services and the information required for their use.

The ‘User Accounts’ database manages all accounts created by users for interaction within the environment. Information contained in these accounts would vary depending on the purpose and the privacy policy of the intelligent
environment. The account would generally include records of previous interactions with the environment and user preferences for information or service delivery, but would not normally include personal details like the user’s name unless this information were required to access a specific service. This user information is stored using an XML-based user-modelling language allowing it to be easily utilised by all of the services required by the user. Service accounts that do not require identity authentication could more easily be copied by the user, and are therefore more suited to the USP system.

The effectiveness of the USP is dependent upon the interface used to manage the user’s accounts and information sharing preferences across potentially large numbers of intelligent environments’ services (Langheinrich, 2001). It will manage the Identity Manager’s privacy preferences, which are responsible for selecting the account to be used in any given intelligent environment, and provide the user with the feedback required to identify potential risks to the user’s privacy. Accounts containing sensitive information would be secured, either with a password or through other means, for example via voiceprint identification. The intelligent environment uses the information within the account and world model to develop a personalised service interaction interface. This personalised interface is then provided to the user to allow access to any required services.

There is a risk when using an environment’s services that users’ real identity may be sensed and applied to their interaction account. These risks are increased the more they use the account, and decrease when more people are present within the environment (that is, the account’s user could potentially be anyone of the inhabitants). This could be compared to the use of Internet chat rooms where the more someone posts under a specific alias, the more likely it is that their real identity may be traced to their alias. To avoid this, user accounts within the intelligent environment should have expiry dates to remove old data from the system (Lahlou & Jegou, 2003). Additional privacy safeguards could be built into the user interface, prompting the user to create new accounts after a default timeframe, or simply through the automatic switching of pseudonyms when in areas of high traffic. This further highlights the criticality of an effective Persona Manager interface.

When a user creates a new account with a service provider, the user has the option of providing service preference and personal information to help personalise the service interface. This can be used to copy all or part of an existing pseudonym/interaction account. This could then be used to manage automatic service interactions or allow the alternating of many pseudonyms to protect the intelligent environment’s service provider from applying all interaction information to the user. The sharing of existing personae between friends or colleagues could further improve anonymity within an intelligent environment. For example, a profile set up to receive specific news alerts or a particular food order could be used by anyone with similar tastes without detriment to the user, but would obfuscate the user’s interactions within a larger population group. This would make it more difficult for the service’s providers to apply an interaction history to a specific user.
To improve this exchange of information, the Service Beacon advertising the service could include a link to an information template that may be used to efficiently populate the new interaction account. These templates are similar to the secured digital templates offered by the Information Service Provider, which could also be used to share information with a service provider. The account information is placed in the ‘User Accounts’ database and used by the intelligent environment to personalise the user’s interactions with any available services. Users can maintain many different environmental pseudonyms, allowing them to effectively choose their required level of anonymity at any given time. This opt-in approach to identity management allows users the flexibility to use these environments as they wish, sharing information about themselves only when given an incentive to do so.

The easily discarded nature of these user accounts means that if a new level of privacy is required, users can simply create a new account, or provide new information to an existing account. The use of accounts with varying details allows the user to provide the minimum information required to achieve their interaction goals, as suggested by the EU disappearing computer privacy design principles (Lahlou & Jegou, 2003). The most effective method of managing these privacy preferences is an ongoing goal of this and other research (e.g. Lahlou & Jegou, 2003; Langheinrich, 2001). Information could also be tagged to prevent its use in certain circumstances, as described in Information Tagging in section 6.4.1.

This system is especially useful for allowing users to interact with different environments based upon their current context. Users could use a different ID for a news delivery service, depending on what configuration of news they require (e.g. professional news, sports, business, etc.), or to manage the payment of goods using different identities (e.g. when using a personal or work account). Using this system, the user is free to develop how they use an environment’s services, and to choose what information they wish to be associated with a given interaction. As User Selected Pseudonyms have yet to be implemented or tested by users, we have not included it within the SPACE architecture.

### 6.5.3 Trust and Reputation Systems

Trust and reputation systems have been suggested to provide additional information to users within ubiquitous computing environments (see section 2.4.6). These servers provide feedback on collective trust ratings that build up over time as the system’s users report on their dealings with an environment or service. Feedback from trust and reputation systems would be presented to users before they interacted with an intelligent environment or service, allowing them to better judge the impact of the interaction on their privacy. The use of these reputation systems would be optional, and different systems might be either open to the public or only available to certain user groups (e.g. users from a particular city, car club or urban tribe).

Trust and reputation systems could either be public or private. Public systems could allow anyone to log in and leave feedback on experiences with intelligent environments, particular services or potentially other users. These
systems would provide democratic feedback on popular systems, and are likely to be regionally specific (e.g. a system might rate all intelligent environments within Australia). Private systems would be systems with an exclusive membership, which may or may not allow voting on the trustworthiness of a particular environment.

A private system might be used for all employees of a particular company (or group of friends) to gather a trust and reputation feedback that is more relevant to them. A paid service might also investigate individual environments and provide feedback based upon a different set of criteria (for example, being able to verify the owner’s digital signature, investigating privacy complaints, etc.). A decentralised system could collect feedback in multiple locations and the reputation feedback might rate local reviews more highly than distant server ratings. Users of such a system might choose ratings from the closest server, or indeed might place more trust in feedback from their home country (which might easily be the case for a traveller in a foreign and potentially hostile land).

Trust and reputation systems in the SPACE architecture are integrated into the user’s interaction interface. Users’ mobile devices would receive the beacons describing the available intelligent environment and service. Their device would then communicate these to the reputation service (via the Internet), and then add any reputation ratings to their environment or services manager interface. A reputation server’s integration into the SPACE architecture is described in Figure 26.

![Figure 26: SPACE Architecture with Reputation Service](image)

Examples of the reputation service integrated into the user or service manager’s interfaces are shown in Figure 27. Both interfaces demonstrate how the reputation feedback might be made available to the users. Essential to effectiveness of these interfaces is the ability to clearly present the reputation recommendations alongside the standard interface, and provide the users with an easy method of providing feedback on the environment or service the user is interacting with. The Intelligent Environment Connections...
screen (shown on the right) shows the results from the user’s two reputation services and allows the user to provide their own feedback. This screen shot shows that different services may well return different results, and it is up to the user to consider the impact of this information. Selecting the **Connect to IE** link would load the User Manager screen to allow the user to select what information is presented to the intelligent environment.

**Figure 27: Reputation Services in the User and Service Manager Interfaces**

Trust and reputation systems will be useful in developing the interactions users have with these new environments. They will allow groups of users to collectively respond to new environments and services and provide feedback for their designers. This allows users to more effectively gauge the privacy risks of sharing personal information with an environment or another user. While this feedback does not provide any additional security, it does allow social forces to impact on the success of an environment based upon the privacy it provides.

### 6.6 Summary and Conclusions

This chapter has described the SPACE architecture, the building block of the ubiquitous computing infrastructure required to provide ubiquitous computing services to all of a user’s everyday environments. The SPACE architecture uses a secure interaction infrastructure, visibility of interaction information and a range of identity authentication structures to support private and secure interaction with ubiquitous computing services. Discussion on the SPACE architecture, and the evaluations carried out to validate its design, are presented in the next chapter.
Chapter Seven: The Application of SPACE to Achieve Privacy in Ubiquitous Computing

7.1 Introduction

The SPACE architecture describes the required support framework for delivering ubiquitous computing services, including secure and private identity brokerage, standardised interactions and service personalisation, and an easily accessible interaction forum that will ideally form the basis for new methods of community interaction. This chapter discusses how this architecture was developed, from the user studies and background literature through to the development of its identity management structures and privacy minimums that support user interaction. This chapter examines issues that occur when integrating intelligent environments into users’ everyday physical environments, the role of the environments in users' communities, and suggests methods to improve the use of intelligent environments by the public.

7.2 Intelligent Environment Architecture

The use of ubiquitous computing technologies carries significant privacy and security concerns that must addressed if a usable intelligent environment is to be developed. User privacy within intelligent environments is heavily dependent upon the legal frameworks, social norms, market forces and architectures in use, along with the ability of users to maintain effective visibility of their personae and control their exchange with the environment. Users’ interactions with ubiquitous computing environments have a significant impact on their privacy and information security.

Users have clearly demonstrated the need for anonymous interactions to protect their identity, as well as the need for interaction flexibility so users can determine which persona is exchanged with the environment or other parties. These interactions, linked with the identity management structures found in the SPACE architecture, provide users with the tools to interact within multiple intelligent environments, whilst allowing users to balance their need for personalised and identifiable services with the risks to their privacy when providing information to the environment.

The evaluation of intelligent environment architectures can occur on multiple levels, from technical robustness and security, to user privacy and perceptions of the worth of such an environment. The investigations in the dissertation have focused on presenting users with a new method of interaction, investigating their privacy concerns and attempting to remedy these concerns with a secure system that can privately deliver ubiquitous computing services.
The SPACE architecture's development into a scalable ubiquitous computing infrastructure must be supported on a global scale to allow users to interact with the environments in a standardised way.

The initial investigations into users' perceptions of information sharing (see section 4.2) described many different influences upon their privacy during an information exchange. This led to an understanding of the types of information users need when interacting with an intelligent environment. The evaluation of a generic intelligent environment (in section 4.3) provided an understanding of the required architectural structures, service personalisation and the technical interactions required when entering an environment. This evaluation led to the separation of the services from the intelligent environment, and to the way personalisation information is managed in the SPACE architecture.

The initial architecture (see section 4.4) was very useful in allowing us to understand the fundamental requirements of an intelligent environment with respect to users’ interaction and service delivery. Our architecture highlighted the need for external identity authentication, raised concerns about the digital fingerprints left within the system that could be used to track or recognise users, and drew us to consider how multiple intelligent environments could inhabit the same physical environments. These requirements were explored in our subsequent user study (see section 4.5), and were added to the requirements for developing a global intelligent environment infrastructure (in chapter five) and developed into the SPACE architecture (in chapter six). The relationship between each research activity is described in Figure 6.

Evaluation of this initial architecture led directly to the need for information beacons to advertise available intelligent environments and services, and to the need for client-side service personalisation. This, combined with the use of random unique interaction IDs and the pseudo-anonymous digitally signed personae, provided the base level of anonymous interaction users require from ubiquitous computing environments. The SPACE architecture provides an interaction environment that allows the user anonymous interaction and service delivery, along with the ability to exchange information with service providers and other users in return for something of perceived value. The effective use of the three identity management structures is essential to the maintenance of users’ privacy whilst utilising these services.

The SPACE architecture uses three identity management structures: the Identity Broker provides high-level, trustworthy identity authentication for service delivery; the Information Service Providers provide third-party digitally signed personae that users can use to share specific parts of their personal information for service delivery and personalisation; and the user’s Personal Domain is the final user-controlled identity management entity that allows users to securely and privately exchange information with other users in accordance with the user’s privacy preferences. Interaction by user study participants with these structures was positive, and their ability to manage and limit user exchanges of personal information was well received.
Security within the SPACE architecture has several redundant layers aimed at eliminating security risks to the user. Initially all interactions with an environment are encrypted using a shared session key provided by the Kerberos key distribution centre or negotiated directly with the environment using its public key. Secondly, all user account numbers are encrypted (with the current date and time) using their destination’s public key. This prevents the account numbers being collected by the intelligent environment or by anyone breaking the communication encryption.

Finally, the destination address of the user’s Personal Domain (provided to the User Register by the user when logging in) is obfuscated using a blind addressing (see section 2.3.2.3) and routing through an Identity Manager. Information security and user’s privacy is therefore only likely to be breached by users exchanging information that should not be exchanged. Users have repeatedly shown a willingness to exchange information contrary to their privacy preferences if offered something of perceived value. This security risk must be addressed via user education in information privacy and interactions with ubiquitous computing environments.

The interaction available between an intelligent environment’s users includes the basic user interaction provided by the environment’s User Register, and through digital interaction communities provided as a service. The interaction that takes place within these spaces is at present similar to basic interaction bulletin boards that are pervasive throughout the Internet. The SPACE architecture, however, seeks to deliver these interaction spaces in a localised, accessible way that promotes easy, casual interaction between the environment’s community members (in short by providing digital third places). These community interaction spaces are examined in detail in 2.2.3, and their place in the SPACE architecture is described in 7.4.2.

The ultimate goal of this research is the private and secure delivery of ubiquitous computing services across all areas of a user’s life. The SPACE architecture provides this service interaction in a way that can be scaled up to allow multiple intelligent environments to overlap in a physical space and share identity management infrastructure. This ubiquitous computing infrastructure, therefore, fulfils the technical requirements for this objective. What is not met is the user evaluation of this infrastructure integrated into users’ everyday lives.

The ubiquitous computing infrastructure would require a significant number of users interacting with numerous intelligent environments before the impact on users’ lives, and their privacy and information security, could begin to be measured. The costs of rolling out such extensive intelligent environment coverage have so far limited implementations to single systems, most often used in laboratory experiments or limited field studies. Furthermore, the interfaces used for presenting the information involved in an exchange have an enormous impact on users being able to accurately judge the impact of an exchange on their privacy. A thorough investigation of user interfaces and the development of enough services to ensure the implementation provided a realistic representation of the environment’s capabilities was outside the scope of this research. The future development path for the SPACE
architecture (and for intelligent environments in general) is discussed in section 8.3.

### 7.2.1 User Register

The User Register provides the connection point for users wishing to interact with other users within the intelligent environment. When connecting to the User Register, users provide any information they wish to share directly to the public and a blind identity account that the environment can use to route information requests to the user’s Public Domain. This system allows users to minimise their exposure to the environment and to other users, whilst still providing a method of interacting with other users.

Threats to the user’s privacy when interacting with the User Register consist primarily of the threat that the user's communications with the environment will be intercepted, and also the threats of being identified by means of the public information the user provides to the environment. All information being exchanged with the intelligent environment is encrypted using either the shared session key provided by the environment’s Kerberos server, or using a session key negotiated directly with intelligent environment (using the environment’s public key, obtained from its description beacon). The encryption used within the SPACE architecture must be strong enough to prevent brute-force attempts at decryption, whilst being simple enough that the user’s mobile device can both encrypt and decrypt responses. The exact key length will increase as the average computational power of the user’s device improves.

All identifiable information that could be used to recognise the user is further encrypted in the SPACE architecture. This prevents privacy breaches in the case of poor message encryption or when a malicious intelligent environment might store information that is contrary to their privacy policies. Identity accounts (for either the identity broker or identity manager) are encrypted along with the current date and time using the destination’s public key. This prevents them from being stored and used for future identification.

The use of randomised unique connection IDs when connecting to an intelligent environment prevents their hardware profiles from being logged and used to recognise the user in the future. The intelligent environment and service discovery mechanisms in use within the SPACE architecture also allow the browse interaction options without requiring the user to reveal any personal information interaction intent. These precautions allow for truly anonymous interaction with intelligent environments on the user's terms. The information users provide to be distributed to the public is perhaps the largest area of concern, particularly if users do not understand who the information will be made available to. These concerns will be addressed with user education and effective user interfaces that allow users to effectively judge the risks to their privacy of any information sharing action.

The use of sensors in intelligent environments cannot really be avoided by the user, which is comparable to the way that people often unwittingly walk into areas under video surveillance. This risk can be eased by excluding the use of...
these sensors in most environments, and by providing notification of this data
gathering in the intelligent environment’s description beacons. This gives
users the option of leaving, modifying their behaviour or simply avoiding
service usage in this environment. This notification is likely to be the best that
we will achieve at present, given the increasing prevalence of the ‘surveillance
society’ in western countries.

The use of ubiquitous computing technologies means that the physical
hardware that runs these environments will often be accessible from within
the environment. Intelligent environments therefore risk being attacked
physically, manipulated to reduce their battery power and bring them offline
(especially for simpler, battery-powered sensors), and could be substituted by
a malicious third party to appear like the environment but provide services
from a rival provider (or simply use the fake services to gather the user’s
personal information). Intelligent environments must therefore be protected
by trusted computing components to prevent them from being hacked and
replaced by malicious third parties.

These vulnerabilities could be overcome by using mains power for sensors
and components, and by using trusted computing components to register an
environment with a third party. This third party could be a simple database or
directory listing all environments within the area, complete with a description,
GPS location and a trusted computing authentication key to confirm its
identity. These directories might go against the spirit of a scalable, easily
extendable architecture that can rapidly change to suit its environmental
conditions. Intelligent environments could still be used without these
directories, their primary purpose being to provide verification that an
intelligent environment is identical to that of the same name that was
encountered last week in the same location.

7.2.2 User Interaction and Personalisation

The interfaces used for interaction with an intelligent environment are crucial
to the user’s understanding of the effects of an information exchange on their
privacy. Users within intelligent environments interact using the Service
Manager and the User Manager, depending on their interaction requirements.
Each interface receives the mDNS beacons describing the available intelligent
environments or services, and uses the XML descriptions to personalise the
user interfaces. This personalisation prevents the intelligent environment from
gathering information on the users, and limits the information that must be
downloaded before the users can make their interaction decisions.

Personalisation occurs based upon two main factors. Users first determine
whether to interact with an environment, and then they decide which services
within the environment they wish to interact with. The SPACE architecture
uses mDNS beacons to advertise the existence of an intelligent environment
and provide more information to allow the user (or their device) to determine
the risks of interacting with the environment. The intelligent environment’s
information collection policy, owner and description could be used to filter out
environments that do not meet the user’s minimum privacy requirements. For
example, the user’s preferences might reject environments run by specific
parties (e.g. known advertisers) or with specific information collection issues (e.g. forced collection of identities, due to either legal or policy requirements).

The SPACE architecture beacons increase the flow of information back to the users, whilst helping users make informed choices about the information that they wish to share with an intelligent environment. The presentation of privacy information before interaction should influence information collection by driving users away from environments with poor privacy protection towards environments with good privacy safeguards. The beacons also allow client-side personalisation on the user’s mobile device, without requiring any information to be provided to the intelligent environment. This personalisation could be further enhanced using a Trust and Reputation system that rates intelligent environments in a particular city or those designed for a particular purpose (e.g. commerce-based intelligent environments). The mobile device could be set to automatically reject (or not show) a system with a ‘privacy friendliness’ rating lower than a given threshold.

Once the user has connected to an intelligent environment, their mobile device collects the service descriptions provided by the Service Beacon broadcasts and selects which ones to display on the user’s interface. This personalisation addresses the invisibility problem of having too much information, designed to blend into the background, for users to usefully recognise and utilise. Service beacons provide the relevant information about an environment or service to the user’s mobile device in a manner that makes it easy to accept or reject, providing lightweight personalisation without requiring users to provide personal preferences to the intelligent environments.

A particular concern of using mobile devices to verify a user’s identity within an intelligent environment is what happens in the event that the device is lost or misplaced. The mobile device can act as a proxy for the user if security is limited to the possession of the phone (using authentication based upon ‘something the user has’). This can be augmented with other authentication mechanisms, namely requiring the user to remember a PIN code (authentication based upon ‘something the user knows’) or submit to a biometric scan (authentication based upon ‘something the user is’).

The level of security utilised should be directly related to the type of identity authentication required. For example, access to the user’s bank account is likely to require a PIN or fingerprint scan, but access to a personalised news service is not. Whilst numerous security protocols and locks could be utilised in securing a mobile device, the safeguards should be proportional to the risk of exposure. In many cases the social mechanisms that surround the handling of another person’s phone (Häkkilä & Chatfield, 2006) may provide sufficient privacy safeguards.

The security of communications with the intelligent environment depends on the handheld’s ability to encrypt data using a shared-session key. This requires a level of computational power that is not available in less advanced handhelds, and may be a barrier for entry into intelligent environments. However, the argument could be made that dramatically more powerful
mobile devices will mitigate this risk (assuming basic Moore’s Law of advancement) by the time of widespread intelligent environment adoption. Additional security on a mobile device could be obtained through the encryption of data on the handheld’s hard drive using trusted computing hardware and protocols. This would be most useful where a device was able to provide access to a classified or high security area, or potentially where the risk of losing the mobile device is considered high.

User Selected Pseudonyms is a method of personalisation that provides the user with a method of manipulating their ‘interaction accounts’ to achieve better service delivery and to improve their privacy. Users will use the system primarily to improve their interaction with services that do not require confirmation of identity, but these services could easily be used with more pseudo-anonymous methods of interaction (e.g. digitally secured templates). The ability to quickly copy part or all of an interaction profile makes it easy for users to maintain similar interaction aliases and share particularly effective interaction pseudonyms with other users. These interaction accounts could be very useful for other users that share the same tastes or course loads, particularly for services that are difficult to use or customise.

The interaction pseudonyms are more likely, however, to be used as shortcuts to obtaining a personalised service. It is much easier to load a profile with the user’s current information requirements than it is to manually set these each time a service is used. Pseudonyms with varying levels of user information could also be set, to allow the user to decide at the point of interaction what balance of anonymity versus personalisation of service delivery is required. The separation of interaction activities also prevents detailed pictures of the user being created, as long as the pseudonyms cannot be matched (e.g. because they have the same personal information). The user’s mobile device must use a new random unique connection ID each time a different service or pseudonym is used to prevent this information collection.

7.2.3 Identity Brokering

Identity brokerage has been in use for thousands of years ever since people have been using paper documentation or tokens to prove their identity to strangers or national institutions. People in the digital age require similar tokens to prove their identity for financial transactions, access restricted services or to identify themselves between service interactions to maintain a consistent and personalised interface. The most important aspect of identity authentication within intelligent environments is the use of graduated personae, each providing different levels of identity, akin to the seven broad types of identity that we enjoy in the real world (described in section 2.4.4).

This graduated real-world treatment of identity allows users to engage in the same interactions that they enjoy in the real world. Intelligent environments’ services will often require users to confirm part or all of their identity, and the SPACE architecture uses three main types of identity authentication. The first is the Identity Broker, which is a trusted third party that can be used to verify part or all of the user’s identity. Identity brokers require users to have an existing identity account relationship before entering an intelligent
environment, and this account will likely be leveraged off existing relationships (e.g. current passports, memberships or bank accounts).

The Personal Domain is an informal user-maintained system that can be used to provide information about the user to external parties (usually other users). The personal domain allows the user to accept information requests from other users without requiring direct intervention by users. This prevents the user from having to personally respond to (potentially numerous) requests for information, and prevents such requests from revealing the user's identity to anyone observing the environment. The personal domain also allows the user to maintain a permanent online presence, which is useful for managing communication and group awareness tools.

Inquiries to the Personal Domains are securely routed through the Identity Manager to prevent the Personal Domain’s IP address from being gathered by the environment, potentially leaving the user open to being recognised between sessions and breaching the user’s privacy. The Personal Domain has the potential to store enormous amounts of information on the user, and any breach of the domain’s integrity (or any of the identity brokers) could be disastrous for user’s privacy. The Personal Domain must be hosted on a secure system that only allows specific connections to handle information requests. Users must also be able to monitor the information requests being served (in real time if possible) and be able to take action if required.

The Information Service Providers allow the user to embrace a third type of identity based upon the provider digitally signing a user’s pseudonym that they know to be true and correct. Intelligent environments then consider the trust they have in the provider before determining its worth as an external identity authentication source. In using these digitally signed personae, users can represent a certain aspect of their identity (e.g. their enrolment status at a local university). These pseudonyms are an essential part of allowing users to obtain services anonymously (or pseudo-anonymously) from an intelligent environment.

Anonymous pseudonyms can safely allow more information to be applied to a user interaction account whilst providing improved service personalisation and increasing the service usage information the environment can retain and reuse (adding value for the environment’s owners). A downside of using these digital pseudonyms is that it can be difficult to predict what information (in what context) future data mining tools will be able to determine about the users. Training users in the use of these pseudonyms would reduce the risks of these breaches of users’ privacy. User Selected Pseudonyms (described in section 6.5.3) is suggested as an interaction method that should be included in the user interfaces to support user selection of the most appropriate pseudonym to meet current interaction and privacy needs.

**7.2.4 Services**

Intelligent environments exist to provide services for users, from providing contextual and environmental information to the user, to the delivery of products and environmental services. Services have been discussed in terms
of the information used to deliver them (e.g. Historical or Real-time) or by the interaction mechanisms they use (e.g. ‘interrupt’ or ‘query-based’ services) (Price, Adam et al. 2005). This research has considered the role of intelligent environments in creating a ubiquitous computing infrastructure, and thus adds the additional dimension of either local or global services (see section 5.2.2). This use of global services requires the intelligent environment to have Internet access, and provide a secure interaction path to these services without gathering information about the user or their service usage.

The types of services provided by an intelligent environment are not, however, as important as the delivery mechanism (predominantly through interaction with a mobile device), the information required of the user and how it is stored within the environment. The SPACE architecture uses service beacons to advertise a service to the greater environment using mDNS messages. These beacons provide personalisation and privacy information to allow users’ mobile devices to personalise their service’s interface. This allows the user’s device to manage the invisibility of service delivery in an intelligent environment without requiring the user to give up personal information without cause.

User information stored within an intelligent environment for service delivery could be reused, breaching the user's privacy. The SPACE architecture uses a tiered encryption method to secure interaction information using trusted computing components. This allows users to encrypt their information on the intelligent environment’s hard drive, preventing its use when the user is not logged onto the environment. Interaction summaries are stored separately to allow the intelligent environment to make use of valuable interaction data to improve their service delivery. The methods of personalisation and interaction described in section 7.2.2, including the use of User Selected Pseudonyms, improve user privacy but reduce the information available to the provider.

The dissertation’s user studies have demonstrated widespread support for the services suggested by this research, particularly in light of the graduated identity brokerage entities in use within the SPACE architecture. These entities allow for anonymous, pseudo-anonymous or verifiable service interaction, which allows users to recreate the interactions that are available in the real world. User must also have a method of removing their information from the service. This gives users confidence in the face of Big Brother and identity theft fears that currently plague ubiquitous computing environments.

The service interface used within the SPACE architecture has a significant impact on the ability of users to interact with services without endangering their privacy. The interface must clearly describe all user information (or which personae) that is exchanged with each service interaction. Other information that is required includes prior interactions with the service, and any additional information available on the service’s owners and privacy policies. The service interface would normally include any third party trust and reputation system’s feedback on the current system, all of which allows the user to consider the risks to their privacy of interacting with the service.
7.2.5 Information Collection

The SPACE architecture uses mDNS beacons to advertise the availability of an environment and its services. These beacons contain details on all information collection activities, which are then applied to the user’s privacy preferences to initially see whether the environment should be offered to the user. The service and environmental beacons can also identify any related legislation or information storage policies that might affect the user’s perceptions of the privacy offered within the environment. These beacons allow users to be notified whenever they enter an environment with unacceptable surveillance or information collection activities, allowing the user to either modify their behaviour accordingly or leave the environment.

The type of information collected matters as much as the resolution and expected accuracy of the individual records recorded. Additional user privacy can be obtained by introducing intentional ambiguity to information records, by reducing the accuracy of information by using high-level data summaries and through preventing information from flowing over natural borders of privacy. The addition of intentional ambiguity, particularly in social systems, allows the user plausible deniability in their actions and locations. This method of ‘social lying’ is necessary to recreate the privacy users enjoy in the real world.

The accuracy of stored data is important for information that might be passed outside of natural borders of privacy. For example, a location system could send the user’s location as ‘145 George Street, Brisbane’ even if the system only requires the user’s current city. Providing this information as simply ‘Brisbane’ would still allow service delivery whilst preventing the user’s actual location from being used for other purposes. This can be equated to the concept of proportionality, which states a system’s utility should be balanced against the impact on the user’s privacy. This trade-off must be clear to the user (essentially a user interface problem), and where possible the privacy minimums built into the system should require the absolute minimum of personal information for service delivery.

Finally, natural borders of privacy must be respected. Environmental services should not be able to pass their information to an external entity without the user’s approval, and global services must be accessed using secure communication paths that exclude the current environment from gathering user information or interaction preferences. This could be achieved using trusted computing tags to prevent data mobility and reuse except under predefined circumstances (see section 6.4.1).

These structures are useful as part of an infrastructure that supports user privacy and information security. However, interactions with intelligent environments are primarily user-driven, with users seeking to exchange information for a service of perceived value. These exchanges mean that the users are ultimately responsible for their own privacy. The SPACE architecture mitigates these risks by using anonymous interaction mechanisms (e.g. blind relays to identity managers, random MAC addresses for environmental and service interaction etc.). The SPACE architecture calls for anonymous services.
wherever possible, and provides easy-to-use service beacons to inform users about the information collection and identity requirements for each service. The visibility the beacons provide should allow social forces to impact on how systems are designed, with those that require superfluous personal information likely to be rejected in favour of those that allow anonymous interactions.

### 7.2.6 Intelligent Environment Comparisons

This section considers the privacy and security protections within the SPACE architecture, and considers how these designs overcome the shortcomings in existing intelligent environments. Predominantly these shortcomings result from the limited scope in the development of intelligent environment. Most intelligent environments are developed to test novel privacy protections methods or environmental security.

The Merino Architecture and the Framework for Intelligent Instrumented Environment are holistic models of intelligent environments that use information abstraction to manage users’ privacy. The interaction model for these environments consists of the user interacting with a single environment, and does not consider that the environment itself could be untrustworthy. In the real world intelligent environments will overlap, be provided by numerous and often unknown vendors and will have to overcome users’ aversions to interacting with pervasive systems that can collect large amounts of information about the user invisibly.

The use of intelligent agents to manage user interactions is rejected. This is due to the inability of intelligent agents to hide their motives in untrustworthy intelligent environments, and users’ general unwillingness to have computing devices or constructs act on their behalf when making information-sharing decisions. The use of intelligent agents in future iterations of the SPACE architecture is considered in section 8.3.4. The SPACE architecture provides the same ability to personalise service delivery based upon the provided user model and abstracted sensor information, but it also considers the greater infrastructure required for interaction with intelligent environments in the real world.

The Gaia OS provides a communication environment that allows anonymous information connections and information routing to protect users’ privacy. The SPACE architecture adds additional user interface and interaction rules around the security provided in the Gaia intelligent environment. The SPACE architecture utilises a system similar to the Mist routers described as part of the Gaia OS. This routing mechanism allows any communication within an intelligent environment to be sent to any location without exposing the message contents or destination. This is essential when interacting with a potentially untrustworthy intelligent environment, and allows users to use their personal domain and global services without exposing the users’ actions. The Gaia OS does not consider user privacy and the interaction methods that would be required for personalised services without providing information to the environment that could be harmful to the user’s privacy.
The MyPlace intelligent environment provides an interaction environment very similar to the SPACE architecture. MyPlace uses a centralised user register to manage users’ interactions, and a publish/subscribe messaging system for information sharing in the environment. This system was combined in the SPACE architecture with new service discovery methods and a logical separation of the environment’s user register and service providers. This allows the user access to services without requiring access to the user register, and affords users complete control over how they access multiple intelligent environments that could potentially cover their everyday environments.

The storage of information within the SPACE architecture was developed through an analysis of the Personal Server and the benefits of storing information on the user’s personal device. The SPACE architecture provides users with numerous storage options that users can use for different purposes. The use of personal domains for online storage and minimal user models to reduce the size of information exchanges allows the SPACE architecture to be adapted to using lightweight mobile devices and (in the future) to biometric recognition for some service delivery.

The iCrafter Service Framework focuses on the adaptability of an intelligent environment and its interfaces to react to changing environmental conditions and add new services as they become available. This is done through the use of dynamic service beacons and flexible intelligent user interfaces that can add new services and data sources as they become available. The SPACE architecture’s use of decentralised service delivery prevents the intelligent environment from logging all service interactions. In the SPACE architecture, the aggregation of services into generic interfaces is done by the service provider (and is not delivered from a central intelligent environment interface server). This design reduces the amount of information the environment can collect about the user, reducing the impact of the service’s use on the user’s privacy.

Service Beacons are used by the iCrafter and PAWS intelligent environments to provide privacy feedback to users on things like data collection and reuse policies before a user accesses a service. This information is essential to allow users to assess the risks of service interaction to their privacy, and was identified in the dissertation’s user studies as essential for promoting user confidence in a service provider. The use of service beacons and interface aggregators improves users’ service interactions through more comprehensive feedback on service providers and through the use of generic interfaces. These structures are adopted in the SPACE architecture.

Trust is built up over time through the observation of previous interactions and an entity, combined with the entity’s reputation. Trust and Reputation systems are therefore especially useful when a user encounters a service or environment for the first time. The Personal Reputation System (PRS) and Pretty Good Privacy (PGP) systems provide feedback on the trustworthiness of an entity, but these systems do not specifically address the other information flow and interaction issues that impact on users’ privacy and security. Trust and reputation systems are built into the SPACE architecture to
provide users with an additional source of information with which to judge the impact of an information exchange upon their privacy.

The SPACE architecture was developed to address the types of interactions that users require with a ubiquitous computing infrastructure (and intelligent environment services). This interaction model provides the anonymous and pseudo-anonymous service and environment interaction identified as important by the user studies and background literature. The SPACE architecture combines the best methods of interaction and service delivery to develop an interaction environment that provides users with complete control over their personal information and service interactions. This architecture allows users to integrate intelligent environment services into their daily lives whilst maintaining their privacy and information security.

7.3 Developing Intelligent Environments

This section examines the development of intelligent environments using the SPACE architecture. It considers problems with the SPACE architecture, and makes suggestions as to how these problems can be overcome. Firstly the effects of the ubiquitous computing infrastructure on the SPACE architecture are examined to determine if an integrated infrastructure supporting multiple environments is possible. Secondly we consider the development of digital community interaction spaces and suggest methods of making these more effective. Lastly this section considers the effect user education and interaction support has upon privacy, security and information sharing habits.

7.3.1 Ubiquitous Computing Infrastructure

The ubiquitous computing infrastructure outlined in chapter five provides a holistic view of how ubiquitous computing environments could be integrated into our everyday lives. Intelligent environments can provide specific services to users within their environment, but their usage becomes more interesting when you consider their role in users’ lives. Intelligent environments developed for specific purposes are likely to overlap, providing users within them several interaction options for many of the environments they encounter on a daily basis. For example, a university campus within a city might have faculty-, university- and city-wide intelligent environments providing services to the same location.

The defining of the infrastructure allows us to consider what global structures are required for interaction with an intelligent environment architecture, and ultimately how we can achieve our goal of providing an Internet-like service architecture to support users in their everyday activities. The SPACE architecture identifies the interaction mechanisms that are used to connect to the environment’s User Register or services. The mDNS advertising beacons used allow multiple environments and services to be served to the same physical environment.

Identity Management entities should be developed apart from the intelligent environments. Identity Brokers should be independent government or financial institutions that can provide trustworthy assurance of the user’s
identity. Identity Brokers should also be registered with a central entity to allow their addresses to be confirmed by intelligent environments. This prevents a user attempting to verify their identity with a fake identity broker (i.e. using the SPAM method of leveraging existing trust by using fake accounts that make the user think that they are dealing with a respected entity, for example using http://www.paypa1.com/ instead of http://www.paypal.com/).

The Information Service Providers are similar institutions that are seeking to provide locally relevant identity confirmation by issuing digitally signed personae. These are likely to be issued by institutions that have good (local or global) reputations, and will normally leverage a pre-existing relationship with the user. For example, a university or employer might issue a signed persona to allow the user easy access to their services. More independent Information Service Providers could use an Identity Broker to verify information before placing it in a signed template. The usefulness of a template relies on the trust the accepting environment has in its issuer, so a template’s usefulness might decrease the further (either socially or geographically) the user is from the issuer.

Each user that interacts with the ubiquitous computing infrastructure requires a Personal Domain to handle information requests and to provide an information repository for global service usage and for the management of group communication tools. This would be served and maintained in a similar manner to a personal webpage, but it is expected that services that provide easily customisable Personal Domains will spring up (similar to Blog websites that provide easily customisable weblogs like http://www.blogger.com/). This would make their development and upkeep much easier, and this would ideally lead to standardised methods for complex interactions to be developed. Each of these identity management structures would be available worldwide, but the trust afforded to ISPs or some Identity Brokers might be diminished by large distances.

Intelligent environments provide local environmental services that users within the environment can connect to. These services might be anything from commercial services to resource and local information discovery to community interaction venues. In addition, other more global services might also be relevant within the environment. The services could provide basic web surfing and information access, or communication tools and other personal services. These services require that intelligent environments have Internet access, but this is also required for third-party identity authentication. This access would greatly increase the value of intelligent environments, making them much more attractive to users sceptical about the benefits of ubiquitous computing environments, although there will ultimately be potential privacy and copyright concerns, and some types of access might be blocked (e.g. access to bandwidth intensive services or adult material).

Intelligent environments must use open non-proprietary standards for user interfaces and the information exchange. This will promote more rapid development of intelligent environments, and should focus developmental activities towards improving information displays (improving the user's ability
to manage interaction information, and therefore their privacy, more effectively) and service delivery (digital communities, global services, etc.). The use of open standards is also more likely to assure users that the intelligent environment they’re interacting with has no subversive processes reusing the user’s information without permission.

### 7.3.2 Community Connectedness

The SPACE architecture could provide local interaction spaces for environments to improve the interaction between community members. But it is not currently clear whether a lack of third places is the primary driver for the disconnection that occurs in modern environments. Although the 'third places' theory has reached a wide audience and has been picked up by numerous companies seeking to attempt to position themselves as a 'third space' for marketing purposes, no statistically significant examinations of the effectiveness of improving community connectedness through the delivery of physical third spaces have been found.

This research does, however, provide a logical starting point to consider the delivery of community supporting services. This section describes the delivery of interaction spaces using ubiquitous computing technologies to overcome the traditional shortcomings of digital communities. The dissertation's ubiquitous computing infrastructure has the dual purpose of supporting community interaction in real third places, whilst providing hosting for localised virtual communities that form virtual third places. Community interaction and social connectedness is supported by providing local information, 'virtual community' interaction spaces and an awareness of users within the current environments. Traditional and ubicomp communication and awareness tools can usefully be utilised to allow micro-communication and the coordination of meetings amongst existing social groups.

Normally digital communities do not provide the necessary conditions for the relaxed interaction that exists in ‘third places’. Soukup (2006) identified that digital spaces attempting to mimic third places normally are not equally accessible, they do not provide a ‘socially levelling’ atmosphere and they often fail to convey a sense of presence to their users. The virtual third places served by the SPACE architecture are accessed via common handheld devices from within our everyday environments.

The existence of the environment is immediately obvious to anyone entering the environment, and this localised access ensures the entire communities have the opportunity to interact with these virtual third places. Furthermore, this localisation allows the rich context of the physical environment to interact with the virtual third place, and this should promote the sense of presence of these environments. Finally, the anonymous interaction possibilities can lead to a sense of playfulness and casualness in the interactions that occur in these places. These factors make the virtual third place more accessible and relevant to the local community if served by a ubiquitous computing environment.
The digital communities and interaction forums provided by our ubiquitous computing infrastructure should be able to act as third places and replace the casual community interaction absent from modern communities. The additional communication and environmental services provided by the infrastructure should also support the interactions that occur in physical third places. These virtual communities meet all the criteria for third place interaction identified by Oldenburg (Oldenburg, 1999) and Soukup (Soukup, 2006), and have the potential to form valuable third places for community interaction.

We expect that these environments will eventually cover the majority of our cities, with smaller localised environments covering our homes, offices, transport networks and public areas. The city-wide wireless networks, which have been extended to provide local information and local interaction possibilities, still provide the benefits of always-on Internet access. These environments follow current projects that provide both free and (faster) subscription-based city-wide Internet access to the public. As our handheld devices gain more processing power and we develop better wireless communication technologies, we move towards always-on access to our friends, family and local community.

This infrastructure will be useful wherever local community interaction is to be encourage, not in places where social connectedness is declining. Future research should examine the use of ubiquitous computing services to localise and host virtual communities and examine the support of specific real third places (e.g. Coffee Shops or Clubs). The types of virtual communities (e.g. Discussion Boards, Chatrooms or MUDs) that will be effective in a given context will be dependent upon the characteristics and preferences of the local community. Of particular interest will be the implementation of this infrastructure en masse, allowing both the evolution of social practices and the adaptation of the technology to make use of this infrastructure in ways unimagined today.

7.3.3 User Education and Interaction Support

The SPACE architecture provides an anonymous interaction infrastructure that allows users to discover and interact with intelligent environments and their services anonymously. The interaction protocols and privacy minimums built into the SPACE architecture are not, however, sufficient to guarantee users’ privacy whilst allowing them to share personal information (or personae) with intelligent environments and their services. The SPACE architecture is supported by the tools that allow users to manage their own privacy whilst interacting within intelligent environments. Central to the goal of managing user privacy is therefore the delivery of an interface that allows a user to manage their interaction intentions and to understand the implications of particular information exchange.

The management of user privacy is highly dependent upon the interaction interface’s macro- and micro-interaction settings, and the user's ability to understand the implications of certain types of information sharing within particular environments. As the information sharing is voluntary (and always
within the user’s defined preferences), the main danger to the user’s privacy is the over-sharing of information by the user. The interaction interface (and the feedback it provides) is therefore an essential part of ensuring that user privacy is manageable when interacting with intelligent environments.

Users must be able to control their mobile device’s interactions with the environment and its services by selecting their current interaction motivation from a simple list. The example in section 6.2.1.1 describes settings ranging from Passive to Active, Anonymous and No Interaction. Another alternative would be the selection of interaction personae that represent the types of information to be shared as a way of controlling what information is passed. User Selected Pseudonyms are presented in section 6.5.3 as a method of controlling these interaction requirements, and this is well received by the respondents of the SPACE intelligent environment architecture user study in section 6.4.2. These tools also require users understand their use, and some user education might be required to improve their effectiveness.

Privacy within intelligent environments is primarily a socially constructed understanding of risk versus reward. It therefore stands to reason that it is essential that the user interacting with the intelligent environment must have adequate knowledge of the influences of intelligent environments, or be able to access this information somewhere within the intelligent environment infrastructure. This means that there is the need for a repository of information on the interaction of intelligent environments that describes the impacts and implications of current and relevant laws, market forces, risks and the value of certain identity attributes (i.e. what information you should and should not share with an untrusted intelligent environment). Much of this information is included in the beacons advertising the existence of intelligent environments, which allows pre-emptive filtering of intelligent environments that do not meet the expectations of the user’s privacy preferences.

Users need to understand the risks associated with leaving their mobile devices vulnerable to theft or hacking, and should understand the information they require to make privacy risk versus reward determinations. Users’ reliance on social practices to protect the privacy of data on their mobile phones will perhaps need to be improved given the additional functionality they will have in the future (e.g. identity management and service interaction). This could be achieved with biometric security locks on their mobile phones, and through software that understands the user’s typical activities and responds to lock the phone when these parameters are exceeded. It is also important that users understand the necessity of these security measures, and this knowledge can support the effective use of security measures within the implementation.

User studies have consistently shown that users are happy to provide personal information in exchange for something of perceived value. The privacy minimums in the SPACE architecture must protect this high-risk behaviour by promoting anonymous and pseudo-anonymous service interaction and by protecting users’ information when it is shared with an environment. This protection is provided by the security of our inter-
environment communication and the use of our various identity management structures that users can provide to protect their personal identity.

Users will need training on the use of our identity structures to provide them with confidence in the encryption and other security methods used, and to prevent them from using the identity tools ineffectively. This training should also include the consequences of using identifiable information in areas designed to hold anonymous information (such as using the persistent use of the same public personal information when logging on to an environment’s User Register), and the more general threats of multi-attributive matching and combinations of personae. This user education requirement is similar to the traditional Internet where the tools and security protocols underpinning information security and privacy are supported by user education against the activities that can circumvent these protections (like sharing passwords or credit card numbers online).

7.4 Summary and Conclusions

This chapter has discussed the ability of the SPACE architecture to solve the privacy and security concerns of users interacting within intelligent environments. The SPACE architecture could form the building blocks for a ubiquitous computing infrastructure that will be able to provide users with services across all of their everyday environments. This chapter has described the interaction of users with other users and environmental services, the necessary identity brokerage, and the impact of the collection of information within intelligent environments.

It has concluded with a list of suggestions that would assist in the implementation of our architecture. These suggestions focus on: the need to provide effective community interaction environments and Internet access to improve the value of the infrastructure; the benefits of tailoring the intelligent environment to its physical and social context; and the necessity of improving users’ knowledge about the security mechanisms in place to ensure adequate security and to prevent widespread violations of users’ security, which will have a negative impact on acceptance of the infrastructures.
Chapter Eight: Conclusions

8.1 Introduction

Intelligent environments lack a scalable private intelligent environment architecture that provides secure interaction with ubiquitous computing services across different areas of the user’s daily life. In order to develop a private and secure ubiquitous computing infrastructure, from which users could access these services, the dissertation set out to solve the following research question:

What type of architecture is required to ensure user privacy and information security within intelligent environments?

This architecture was designed to overcome the privacy concerns users have with the nature of ubiquitous computing environments and, in doing so, developed the required infrastructure to secure users’ communications and service interactions. This was accomplished by further considering the research sub-questions, also outlined in section 3.2. These sub-questions include:

• How do intelligent environments impact on a user’s privacy?
• What type of security design is required to ensure the integrity of user data?
• How do users interact within an intelligent environment?
• What type of design is required to allow users seamless interaction between multiple intelligent environments?

To accomplish these goals, the dissertation has examined all recent and foundational research on user privacy, including users’ perceptions of information sharing, and the impact of ubiquitous computing technologies, regulation and the environment on user privacy (and their perceptions of privacy). The results from this analysis and the dissertation’s user studies were combined to define the required components of a ubiquitous computing infrastructure that could support multiple environments. These requirements were combined to create the SPACE architecture (described in chapter six), and the iterative design process used further user studies to improve its privacy and security protections.

This chapter concludes the dissertation by examining its contribution to the field of developing ubiquitous computing environments, the limitations of this research, and the research directions that could be profitably investigated by future researchers building on this work. Future research that is examined includes the concept of the disappearing computer and its impact on the SPACE architecture, the integration of the SPACE architecture into our everyday environments and communities, and the use of intelligent agents to act as proxies for users within intelligent environments. This chapter
concludes with an examination of the current outlook for ubiquitous computing environments and technologies in our everyday environments.

**8.2 Contribution and Results**

The dissertation developed the Scalable Privacy Aware Communication Environment (SPACE) architecture that users could use to safely interact with an intelligent environment's users or services. The SPACE architecture provides an anonymous interaction framework with privacy protections based upon the requirements developed from the analysis of existing research, the iterative development and testing of the resulting architecture, and the results of field studies with users investigating the interaction with intelligent environments. Intelligent environments developed using the SPACE architecture provide anonymous interaction spaces and a range of identity providers to authenticate the user to the service providers based upon their interaction needs.

This dissertation also developed, in conjunction with the SPACE architecture, the requirements for a ubiquitous computing infrastructure to support the intelligent environments. This infrastructure would allow the multiple SPACE architecture implementations to be served from one physical location, and provides the range of identity providers required to give users the interaction (and identity authentication) capabilities they enjoy in the real world. This dissertation therefore provides the infrastructure and architecture requirements to implement intelligent environments across user’s everyday lives.

The fundamental privacy and security underpinnings of our intelligent environment architecture are described in the next section. This is followed by a description of the SPACE intelligent environment architecture and an examination of how the architecture could be used to provide the desired ubiquitous computing infrastructure that could provide services to users across most of their daily environments. This section finishes with an evaluation of the limitations of our research results and the methodology used.

**8.2.1 Privacy and Security in Ubiquitous Computing**

Privacy is a socially constructed concept. Current concepts of privacy have evolved from ‘the right to be left alone’ or protection from the use of unauthorised photos in newspapers (Warren & Brandeis, 1890) to the more modern “protection against unreasonable or burdensome intrusions” (Lessig, 1999, p. 148), or the act of keeping information secret from all but those who are authorised to see it (Menezes, van Oorschot & Vanstone, 1996). Privacy is no longer the exclusion of collecting information about the user. It is about users having control over this information collection and exchange. These perceptions of privacy are changing over time as users become accustomed to the surveillance society we live with in modern times. The goal remains in spite of this (potential) acceptance to identify risks to users' privacy and allow users to make informed decisions about their interactions.
Privacy in this case remains the effective consideration and control of information exchanges with the environment and the ability to obtain services whilst maintaining users’ privacy preferences. Adequate feedback about users' interaction activities, including with whom they are sharing information and what this information will be used for, is required for effective decision making about the impacts of an exchange upon the user's privacy. Feedback on data collection should ensure that the user has comprehension, consciousness, control and has given consent of all information collection activities.

Privacy within an individual interaction is broadly reliant on the prevalent architecture, market forces, social norms and laws that govern an area. Global privacy legislation is varied, but our environment is designed to work within all these regulations. Privacy within intelligent environments should, as far as possible, provide feedback about local conditions. For example, the environment should communicate relevant legislation, market forces and architectural design information to users to allow them to make up their mind before interaction decisions are made. Where possible the user's information flow must be limited to prevent the crossing of natural borders of privacy and to ensure more information flows to the user than from the user. Privacy decisions made about one area may not necessarily hold in other areas, and users must understand what environments (and legislations, architectures and information reuse regimes) they are interacting with.

Pseudonymous and anonymous interaction with intelligent environments has great potential for managing users’ privacy within intelligent environments. To accomplish this, users must have complete control over how they are presented to the environment, nominally called the persona or ‘face’ they wish to be recognised as. The management of this identity exchange and persona interaction is critical for the development of new forms of interaction and to allow users to understand and interact safely with intelligent environments. This management is integrated into the SPACE architecture’s persona manager (see section 6.2.1.1), and an extension of this interface is described as User Selected Pseudonyms (see section 6.5.3).

User privacy is heavily dependent upon adequate security being available to provide confidentiality and integrity to communications within the environment. This prevents the disclosure of users’ personal information to the intelligent environments and other users, thus safeguarding users’ privacy. To maintain this security, the intelligent environment will require either an encryption key manager to provide interaction session keys to all participants, or the use of public/private key pairs for the exchange of session keys for message encryption.

The dissertation's user studies and initial architecture highlight the need for effective user feedback on information exchanges, and for effective, secure and private identity management to assist in users’ service interactions. Identity management entities within our ubiquitous computing environments should allow the graduated levels of identity that we use to interact with the real world, from pseudonyms without identifying information to verified names and financial details. Users also require a private method of accepting
information requests about themselves if user interaction with the intelligent environment is to be supported. Anonymous interactions should be possible at both a service and network interaction level.

Personalisation within intelligent environments should, where possible, be done on the user’s device, to reduce the user’s personalisation preferences from being collected by the environment. A lightweight interface is required to manage the potentially huge number of environments and services that could conceivably cover a single area. The effectiveness of the interface used by users to manage their environment and service interactions will ultimately determine how effective users are at managing their own privacy. The security for the mobile device providing this interface is therefore also crucial. These design requirements have shaped the SPACE architecture (see 8.2.2) and structures required in the greater ubiquitous computing infrastructure.

8.2.2 Intelligent Environment Architecture

The SPACE architecture was developed by examining existing intelligent environments and combining the interaction and security design components of these environments with our research and other existing research on user privacy within intelligent environments. The SPACE architecture uses a secure interaction space and three methods of exchanging identity information to eliminate the threats to user privacy that threaten to destroy users’ confidence in ubiquitous computing environments. Our architecture uses third-party identity management and a distributed design to allow the creation of a ubiquitous computing environment that might consist of overlapping intelligent environments, and which will likely provide support services to most of the user’s everyday environments.

Identity management within the SPACE architecture requires three types of identity authentication for different purposes. Identity Brokers provide a central identity authentication service similar to the role of government passport issuing departments. Identity Brokers can be used to confirm service access, provide user information (e.g. name or address) or to validate access to an interaction account. Information Service Providers can digitally sign user information templates that can be provided to third parties as a way to prove aspects of the user’s information. The signed personae can be used to provide interaction or demographic information to a service without requiring users to give up private personal information.

Finally, users can maintain their own Personal Domain, which acts as a proxy for users to handle information requests (and manage global communication tools or services) in accordance with their privacy preferences. The Personal Domain can accept information requests from other users and provide connection to the user’s mobile device in some circumstances. Users can use these facilities to recognise their friends within intelligent environments, provide public information about themselves (which could lead to novel types of service delivery) and reduce the interaction overheads for their mobile device.

The SPACE architecture was developed using an iterative approach, with the initial architecture undergoing two user study reviews to ensure the
environment had the necessary privacy precautions. These precautions included the use of random MAC addresses and blind information relays to protect identifiable user attributes, allowing users complete control over the information exchanged to receive environmental services, and securing of information stored within intelligent environments using trusted computing encryption. This architecture is secured using a Kerberos server for key exchange, and locally using the PGP system of exchanging a session key using asymmetric public/private key pairs.

8.2.3 Ubiquitous Computing Infrastructure

The dissertation commenced the development of our intelligent environment architecture by considering the types of interactions users required with intelligent environments, and then designing the types of infrastructure required to support these interactions. Chapter five describes the required attributes of this ubiquitous computing infrastructure. These requirements were integrated into the SPACE architecture, and this architecture therefore provides the perfect interaction infrastructure from which to provide personalised and secure service delivery.

Intelligent environments developed using the SPACE architecture could use the same identity management structures, user interface and technical infrastructure, and could be linked together to form part of a ubiquitous computing infrastructure. The common identity structures, interaction interfaces and mechanisms and global services should reduce the effort required to develop intelligent environments, allowing more effort to be put into the delivery of usable and valuable services. These entities also provide a method of instilling shared values between the service users and providers, increasing trust within the environment, and provide an avenue of recourse in the event that a user's trust is broken.

In developing a secure and private architecture for interacting with intelligent environments we have developed a ubiquitous computing infrastructure that could cover people’s entire lives. Users could utilise this architecture to not only privately access intelligent environment services, but to remain connected to their personal networks of friends and family, and to interact with their given environment and foster community connectedness. By moving beyond the more basic ubiquitous computing services, our architecture considers what the greater purpose of a ubiquitous computing infrastructure should be.

Obviously there is great potential to support users’ everyday lives with ubiquitous computing services. Intelligent environments can provide directions, local information and m-commerce opportunities that are integrated into cities’ transportation networks, news services and access to communication channels, both within the environment and across the Internet. But these environments could also be useful for supporting the interaction of users within their community, and conceivably provide accessible and localised digital third places that embody the feel of a community and promote community interactions similar to their non-digital counterparts.
8.2.4 Limitations of Research

The dissertation was limited by two fundamental challenges that frustrate the development of such an all-encompassing view of the way users interact with their environment and ubiquitous computing environments. Firstly, the technology that these environments utilise remains just beyond the grasp of today’s users, and therefore any interactions with the developed intelligent environments will be more novel than an integration of a new technology into the users’ existing everyday environment. The novelty of the environment’s interfaces could perhaps overshadow design flaws that would affect the success of the interface (and the environment) in everyday use. This was addressed by the use of questions investigating users’ privacy perceptions of information exchanges and the types that will be serviced from intelligent environments.

Further challenges are presented again by the theoretical nature of most intelligent environments in current everyday environments. To be effectively evaluated, intelligent environments need to be integrated en masse within an environment and utilised by significant populations using the environment as they go about their everyday tasks. In particular, the concept of a ubiquitous computing infrastructure providing services to users wherever they are needs to be validated by the integration of multiple intelligent environments covering different areas of the users’ lives (e.g. home, office, transport networks, shopping centres, etc.).

The necessarily expansive scope investigating users’ perceptions of a new technology concurrently with its development caused difficulties in the bounding of the research problems and identification of the research priorities. The technical implementation of the architecture was developed after extensive user studies that investigated users’ perceptions of information sharing and privacy within ubiquitous computing environments. But investigation of privacy-related behaviour is often complicated by users’ tendency to over-report their privacy preferences, or, stated another way, the tendency of users to give up personal information or their privacy for goods or rewards of relatively little value. This may put our research in the position of suggesting more stringent privacy controls than might be strictly necessary.

This concern is acknowledged, but privacy research consistently recommends that a minimum level of privacy protection be built into these types of environments to protect user privacy. The dissertation’s ubiquitous computing infrastructure is also designed to be implemented globally using the same architecture, and this suggests that our system must adopt the most stringent privacy controls to make it palatable to all audiences and respect all privacy regulations. This architecture will be an effective starting point from which to implement an intelligent environment over a wide area (and large population) in order to study users’ actual privacy perceptions and usage behaviours.

This research used a combination of Activity Theory, Design Science and Critical Heuristics. Activity Theory provides a development framework based around the design of a new interaction method or task based upon a user’s
context and available tools. Design science is concerned with the development of artefacts to obtain interaction or processing goals, and provides the development framework that the Activity Theory lacks for tool development. (In this case the tool is our intelligent environment architecture that users use to interact with environmental services.) Critical Heuristics was adopted to improve the analysis of the environmental impacts on the activity under study and the artefact’s design.

These research activities are ideally suited for this development. The interaction with intelligent environments and their services is a new area that needs to be better understood to allow the development of an infrastructure that provides users with appropriate identity support and privacy safeguards. The analysis of the problem with Activity Theory and Critical Heuristics developed this understanding and allowed the development of appropriate interaction requirements. The design science guidelines helped further focus the development, evaluation and communication of the architecture’s design. But the methods used lack clear methods of assessing a design with users and within a specific interaction environment. This lack of user grounding was addressed with user studies and more basic user surveys.

The user studies carried out on these environments were a mix of laboratory and field experiments aimed at understanding the use of an intelligent environment in natural settings. This work would be more effectively examined using field studies investigating intelligent environments implemented into the user’s natural environments. The dissertation’s research by necessity adopted some aspects of a laboratory test, as the resources and time available to implement wide-scale intelligent environments with real user supportive services were unavailable. The user studies were limited in this way, but considering the representativeness of the user population (addressing early technological adopters) and the user-reported usefulness of the services provided in the user studies, the dissertation argues that these user studies were useful in identifying interaction requirements that are valid for a majority of future intelligent environment users.

The lack of real-world services available meant that our environment had to control the service delivery, something common in laboratory experiments that can lead to a lack of realism and low external validity. To overcome this, user studies were conducted within the user’s natural environments, and the services were appropriate to the audience and the setting. This localisation is common to field studies, and it presents a realistic representation of users’ perceptions and activities within genuine intelligent environments. This provides our research with a high level of external validity, improving our ability to draw valid conclusions from our user studies.

Despite these research limitations, the dissertation clearly evaluated and described the interaction requirements for users to privately and securely access ubiquitous computing services from their everyday environments. These interaction requirements and the results of the dissertation’s user studies were integrated into the development of the SPACE architecture. This intelligent environment architecture provides users with anonymous methods
of interaction that allow users to seamlessly move between intelligent environments for service access without endangering the users’ privacy.

8.3 Future Research

The suggested benefits of intelligent environments lie in the development of environments that can anticipate and react to users’ needs and deliver services that provide value. But the goal of providing these environments is still several years away. Intelligent environment prototypes are currently limited to discrete environments with a limited number of users. Environments that cover larger areas and more diverse users are required to study how these environments can handle large crowds and interactions between masses of people.

Services provided by the intelligent environments need to be developed to ensure they provide valuable additions to existing environments. Finally, more work is required to develop effective methods of integrating these environments into the community, building on existing infrastructure and users’ devices (e.g. PDAs or mobile phones). This section examines the future of the disappearing computer (or ubiquitous computing), social integration and implementation of the SPACE intelligent environment into real-world environments, and the use of intelligent agents within the ubiquitous computing infrastructure.

8.3.1 The Disappearing Computer

The ultimate goals of ubiquitous computing calls for computing devices to move into the background and no longer remain the focus of our attention. Intelligent environments seek to accomplish this by using ubiquitous computing technologies to unobtrusively gather and provide information and services to users without obvious computing interactions. However, today’s intelligent environments do not go far enough towards achieving this goal. Intelligent environments still rely on existing mobile devices or shared environmental infrastructure (e.g. public displays etc.) for interaction with the environment.

The goal of disappearing computers might be better accomplished by removing the computing interaction tools that exist between the user and the environment. The use of biometrics would make the identification of a user without a computer easy, but would raise numerous questions on how identity would be utilised, secured and obscured. A design with sufficient security and privacy guarantees would allow users to interact with their environment directly. The environment could recognise a user (e.g. via a face scan) and subtly alter the environment based upon their expressed preferences.

A central information store (like the Personal Domain in our architecture) could be used to store personal information and handle requests from an intelligent environment or other users. With access to a central identity repository, an environment could identify a user each time they entered an environment, but they could easily be denied access to the user’s name or
other identifying information. Similar access could allow services such as using a fingerprint reader to bill a telephone call to a user’s account without the local environment knowing who the user is. The effective use of biometrics in the SPACE architecture raised complex privacy questions, and is examined in more detail in section 8.3.5.

The disappearing computer age is upon us, and the environments developed today will impact on the form, impact and acceptability of the environments of tomorrow. Intelligent environments have the ability to greatly enhance the lives of an environment’s users and greater community, but they also have the potential to greatly increase surveillance of a user’s activities and reduce or even eliminate their privacy. It is essential for privacy and security to be an integral part of their design and development, or these environments will be at best avoided, and at worst damaging to the community. Expanding the SPACE architecture to use these insecure public interfaces (and other interaction devices) requires more research investigating their impact on user privacy, users’ perceptions of security and service delivery.

8.3.2 Social Integration and Development

The social integration of intelligent environments is an interesting yet difficult proposition. Ubiquitous computing environments have significant privacy concerns that turn users off their use, and problems with identity theft, Internet scams and fraud are increasing. Any intelligent environment that is deployed within a community environment must have sufficient privacy and security safeguards to ensure its users are not victims of any of these annoyances. The SPACE architecture does provide secure interaction and effective identity management structures, but communicating this to users with rudimentary technological skills might be a challenging prospect. This reinforces the need for user interfaces to effectively communicate the privacy implications for an information exchange.

Today, more than ever, people are being brought closer together with mobile and email based communications devices, the Internet and more functionality being available for users’ phones. Students entering the workforce today have spent most of their lives using these types of technologies, and they are more likely to embrace useful, pervasive computing devices than ever before. When this is considered in light of the saturation of mobile phones in western communities, it would seem that an infrastructure exists that could be used to deliver intelligent environments to large portions of the community. But in order for the mass adoption of intelligent environments to come about, there need to be more useful services available, and the security and privacy protections within the architecture must be effectively communicated with users.

The use of ubiquitous computing environments that cover large areas of our lives is still quite a few years off. Intelligent environments that provide specific services are becoming increasingly popular in research, but their general usefulness is questionable. Intelligent environments that support communities should provide an interaction framework that third-party providers can use to provide valuable services. This framework is likely to
evolve as the relative merits of each aspect of our SPACE architecture are evaluated under natural conditions, and potentially as new structures to provide assurance to users are developed or retooled. For example, the use of local lists maintaining the digital signatures of intelligent environments to ensure they are not replaced by malicious third parties might not make sense in one environment, but may need to be expanded in another. New methods of interaction between users might also be developed, for example, users might be able to donate the services of their mobile devices to split interaction problems between all users within the environment (similar to how the SETI @ Home project splits up its computational calculations between idle computers).

An important aspect in the social integration of our ubiquitous computing infrastructure is the consideration given to our digital communities that seek to support and supplement the 'third place' interaction spaces missing from modern western communities. Firstly, research needs to be focused on whether these environments can provide the social and technical accessibility and presence required to enable the same types of community interactions provided by third places. This would include an evaluation of the best interaction environments (e.g. discussion boards, chat rooms, multi-user domains, etc.) to promote community interaction and connectedness.

Additional research should focus on the way communities use the interaction and environmental information services to manage community interaction throughout the infrastructure. The research should investigate the differences in how different user groups interact with the infrastructure, including how this affects their interaction with the greater community and what services they find most useful. The difficulties here are obviously the deploying of an intelligent environment that covers such a wide range of users. This environment could leverage an existing technical infrastructure, like the GSM telecommunications network, with interactions provided to users’ mobile phones. This would require a significant educational campaign on privacy and the security available within the intelligent environment before users are likely to interact with the system en masse.

**8.3.3 Community Integration of Intelligent Environments**

More work is required to test the effectiveness of the SPACE architecture in users’ everyday environments. This work should include: the investigation of services that can be profitably served to users via mobile or ubiquitous computing devices; the mass use of embedded devices in urban environments; methods of educating users about their privacy rights, technical security and privacy protections; and methods of integrating intelligent environments into user communities.

The integration of intelligent environments will likely be done piecemeal as technological advances allow the delivery of anonymous services to mobile phones and PDAs, and as new services (or ‘killer applications’) drive user interest in locally provided information and services. Services that require identity confirmation will most likely evolve to use mobile phone accounts and traditional identity relationships (e.g. government-issued passports or ID
cards), but there will also be a drive for anonymous or pseudo-anonymous service interaction and links with online identity firms (e.g. OpenID). Users will require education on how identities are created, protected and shared.

Given the increasing acceptance of surveillance cameras in our cities, and to a lesser degree the filtering or trawling of Internet traffic for illegal activities, it will be interesting to see if users become more or less accepting of surveillance systems. These changing perceptions will obviously impact on any intelligent environment development, particularly if the privacy protections like those found in the SPACE architecture are not clearly communicated to the public.

Once implemented on a wide-scale, the effectiveness of the SPACE architecture in protecting user privacy and information security can ultimately be established. This evaluation requires a representative sample of potential users to be included, must provide useful services that users will engage with in a natural manner, and must investigate the possibility that the substitution of intelligent environments with malicious entities would be occasionally expected in the real world.

### 8.3.4 Intelligent Agents

Intelligent agents are semi-autonomous software agents that are capable of carrying out high-level interaction instructions. Intelligent agents could take over the user’s interaction with intelligent environments’ services by adhering to the user’s privacy preferences and interaction goals, using feedback to help the intelligent agents learn to improve their interactions. This would allow users to have multiple intelligent agents supporting their casual interaction with intelligent environments. An example of this would be a news and traffic reporting agent that connects with each intelligent environment the user comes across to download the latest news and local traffic conditions. More advanced teams of agents might support all information needs for the user and coordinate this information with selected peers.

Intelligent agents have numerous privacy concerns when they are exposed to untrustworthy hosts. Users have no way of knowing whether the interaction motivations, personal information and privacy preferences contained within the agent would be compromised, and if so what the effect of such a breach would be. If intelligent agents are to be integrated into our ubiquitous computing infrastructure, then these privacy and security questions must be solved. Users must also overcome the trepidation demonstrated in our user studies for allowing their computing devices to share information without their explicit consent.

There exists the possibility that intelligent agents could be used to manage users’ interactions with intelligent environments and their information services. Specifically, intelligent agents could be used to automate many of the information-collection activities that we engage in on a daily basis, like the tracking of financial data and news reports, to help manage the collective awareness within a social group by providing (user-designated) automated updates to other members, and to provide a seamless integration method to
interact and gather feedback on the user’s community. Intelligent agents would not be able to interact with the intelligent environment infrastructure in a different method from the user, but might be able to understand the user’s preferences well enough to act on their behalf without threats to their privacy or information security.

8.3.5 Biometrics

Biometric technologies could be integrated into the SPACE architecture in two ways. The first and easiest way to integrate biometrics is the use of biometric sensors to secure the user’s mobile device. This would provide extra security for the user’s mobile device without substantially altering the architecture. Biometrics are already being utilised to secure mobile computers. Fingerprint scanners that lock and unlock laptops and PDAs have been available to the wider public since 2004 (e.g. iPaq hx5550). Numerous other biometric devices will likely be adopted as their accuracy and security is improved.

These systems could address the need for additional, non-burdensome security for mobile devices to supplement the social rules that protect the information held on another person’s mobile device. These systems could also be useful backup security checks that might activate when the phone or PDA is being used in a manner outside its normal use parameters. For example, a phone that is normally only used in Brisbane, or one that doesn’t normally connect to intelligent environments might require a fingerprint scan to prevent it locking down when either of these rules are exceeded (and thus giving the phone reason to believe it may have been stolen).

Intelligent environments could also use biometrics to recognise users and to allow users to maintain consistent interaction throughout multiple visits to an intelligent environment. This would move the environment away from user’s interacting with ubiquitous computing with their mobile device, and towards the use of automatic user recognition and tracking, similar to that seen in our Minority Report example (Dick & Frank, 2002) in section 1.1. This second use raises many potential privacy problems that occur when users are automatically tracked and information on them is automatically gathered and inferred.

An intelligent environment that uses biometric recognition could be developed to reduce the environment’s access to their personal information. For example a user might set up an account with a third party to allow the recognition of the user across multiple settings (so they can retain interaction preferences or access the same service) without the third party releasing any personal information. In this case the intelligent environment would know that the persons designated ‘A001’ had returned, but not who that person was. Intelligent environments could use this information to provide personalised service to users by recognising them from previous scans. Interaction with services that use this type of identification could use either voice interaction or public displays. The use of public interfaces however causes additional privacy concerns relating to the displaying of private information on the public screens.
In another example a takeaway store might use facial recognition scans taken from a security monitor to recognise users from previous visits and provide them with personalised service. The camera could, for example, track the user’s location, and, when they are at the front of the queue, their normal order (or previous interactions) could appear on the server’s register. A system using this type of user recognition should adopt a ‘privacy minimums’ strategy, only storing information required to deliver the service. Furthermore, the system could avoid other privacy problems by only storing information within the store environment (and not allowing photos of customers to be removed from the system).

Biometrics may provide useful interaction mechanisms in the future, and their ability to provide effective, easy to use security is obvious. But the ability to use them to identify users within an intelligent environment, without presumably giving the user the ability to interact anonymously, combined with their public interaction methods (public screens, voice interaction, etc.) currently make their use infeasible. Further research should investigate effective methods of handling user privacy whilst using biometric recognition within intelligent environments. The viability of these architectures, and their ability to reassure their users of their privacy and information security, must be central to this research investigation.

Outlook for Ubiquitous Computing

Ubiquitous computing technologies are increasingly being implemented throughout our world. Current applications use RFID chips to label and track library books, household objects and shipping containers, and prototype systems use embedded environmental sensors to build up incredibly detailed real-time pictures of an environment. This technology is effectively invisible, and allows new services to be developed to support users in existing environments. But this invisibility of information collection and reuse has caused great concern amongst its intended users.

Intelligent environments have great potential to deliver personalised, context-aware ubiquitous computing services to users in all of their everyday environments. This potential is under threat of never being implemented due to a wide range of user privacy concerns arising from years of surveillance and not trusting Big Brother-like organisations and governments. Intelligent environments developed with the SPACE architecture could easily form a greater ubiquitous computing infrastructure that protects users from unnecessary privacy intrusions. The SPACE architecture allows users complete control of their personal information, and affords them control of how they represent their identity across multiple intelligent environments and services.

The dissertation has utilised the evaluation of current design literature, an iterative development process, and user studies that inform on users’ perceptions and interaction requirements within intelligent environments to develop a privacy and security-aware architecture. This SPACE architecture uses third-party identity management, secure key-exchange and management, and user-controlled personalisation and interaction to provide the required levels of security and information privacy. With this architecture intelligent environments could provide useful ubiquitous computing services across users’ lives.
Future research into these environments should involve their implementation and adoption by large user groups. It will be these community-based implementations that will begin to reveal how users will make use of this service infrastructure, and lead to new forms of social interaction and service usage. These environments will emerge as mobile devices become more capable, as users become more technically savvy and as user groups gradually accept the benefits of interacting with these environments. The dissertation provides the foundations for an interaction infrastructure that provides services to users without threatening their privacy or information security, and provides an interaction forum for the delivery of new intelligent environment services and community interaction spaces.
References


Adams, A. 2000, 'Multimedia information changes the whole privacy ballgame', in *Computers, Freedom and Privacy*.


Brands, S. & Paquin, C. 2010, U-Prove Cryptographic Specification V1.0 Microsoft Corporation


Clarke, R. 1998a, 'A History of Privacy in Australia: Context.'.


Clarke, R. 1999b, 'Internet Privacy Concerns Confirm the Case for Intervention', *Communications of the ACM*, vol. 42, no. 2, pp. 60-7.


References


Cunningham, J.B. 1997, 'Case study principles for different types of cases', *Quality and Quantity*, vol. 31, pp. 401-23.


*The Equator Project*, <http://www.equator.ac.uk/>.


Hitchens, M., Kay, J. & Kummerfeld, B. 2004, *Secure identity management for pseudo-anonymous service access*, TR546, Department of Computing, Macquarie University; School of Information Technologies, University of Sydney, Sydney, Australia.

HITLab, *Human Interface Technology Laboratory New Zealand (HIT Lab NZ)*, <http://www.hitlabnz.org/>.


References


Kay, J., Kummerfeld, B. & Lauder, P. 2003, 'Managing private user models and shared personas', in Workshop on User Modelling for Ubiquitous Computing, Pittsburgh, PA, USA.


References


Leonhardt, U. 1998, Supporting Location-Awareness in Open Distributed Systems, Department of Computing, Imperial College of Science, Technology and Medicine, University of London.


Risborg, P. & Quigley, A. 2003, 'Nightingale: Reminiscence and Technology - From a user perspective', in *Australian Web Accessibility Initiative (OZeWAI 2003)*, La Trobe University, Victoria, Australia.


Segall, B. & Arnold, D. 1997, 'Elvin has left the building: A publish/subscribe notification service with quenching', in *AUUG97*, Brisbane, Australia.


Weiser, M. 1994, 'The World is not a Desktop', ACM Interactions.


Zimmermann, P.R. 1995a, PGP Source Code and Internals, MIT Press.

