USER-CENTERED AWARENESS AND CONTROL OF PRIVACY IN UBIQUITOUS COMPUTING

BASTIAN ALBERT JOSEF KÖNINGS
aus Goch

DISSERTATION
zur Erlangung des Doktorgrades
Dr. rer. nat.
der Fakultät für Ingenieurwissenschaften, Informatik und Psychologie
der Universität Ulm

Institut für Medieninformatik
Fakultät für Ingenieurwissenschaften, Informatik und Psychologie
Universität Ulm
2015
AMTIERENDE DEKANIN / ACTING DEAN:
Prof. Dr. phil. Tina Seufert

GUTACHTER / REFEREES:
Prof. Dr.-Ing. Michael Weber (Universität Ulm)
Prof. Dr. rer. nat. Frank Kargl (Universität Ulm)
Prof. Dr. rer. pol. Sarah Spiekermann (Wirtschaftsuniversität Wien)

TAG DER PROMOTION / DAY OF DEFENSE:
26. Mai 2015

Bastian Albert Josef Könings
User-centered Awareness and Control of Privacy in Ubiquitous Computing
Doctoral dissertation

2015. Some rights reserved

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/. Exceptions from this license may be granted by the author upon request.

This document was typeset in \LaTeX using the typographical look-and-feel classicthesis developed by André Miede (http://code.google.com/p/classicthesis/)

Icon credits: PICOL-icons (http://www.picol.org/) used with permission from Melih Bilgil.
Dedicated to the loving memory of

Sophie Gertrud Könings & Artur Günter Hinderberger

ABSTRACT

The vision of Ubiquitous Computing (UbiComp) foresees a future of context-aware smart environments which unobtrusively and invisibly support users in their daily activities. Those smart environments are characterized by the integration of sensing and interaction capabilities with almost ubiquitous inter-connectivity. These characteristics of UbiComp systems pose several risks to users’ privacy. Users often lack awareness about a system’s capabilities to gather data or to intervene in user activities, or are even not aware of the system’s presence. Furthermore, controlling such systems according to individual privacy preferences constitutes another critical challenge.

This work addresses these privacy issues by proposing a user-centered framework to support privacy awareness and control in UbiComp. To cope with the privacy challenges of UbiComp systems, the concept of territorial privacy is defined, which enriches the dominant information-centric view of most privacy research with physical aspects. Thus, territorial privacy refers not only to observations that affect users’ privacy by gathering personal information, but also to disturbances that affect users’ privacy by undesired physical interventions or interactions.

From an access control point of view, territorial privacy includes access to personal information, physical access, and access to a user’s attention. Based on this concept of privacy, a territorial privacy model for UbiComp is proposed. The model allows to capture which entities affect a user’s privacy, how and why. The graph-based approach of the model further allows to identify dependencies between entities, and consequences or conflicts of potential control decisions.

On the system level, channel policies are proposed to allow the instantiation of the model. Channel policies provide information on an entity’s privacy implications and provide references to available control points for privacy enforcement. Different optimistic and pessimistic mechanisms to support the discovery of channel policies and the control of privacy implications have been developed in five discovery and enforcement modules. The modules address the different characteristics of UbiComp systems as well as the different settings and conditions of a user’s environment. The modules have been implemented as prototypes and evaluated for their technical feasibility and effectiveness. The results confirm the applicability of the different discovery and enforcement approaches.

To complement these discovery and enforcement modules, a user interface for user-centered privacy management has been developed in an iterative design process. This interface maps an instantiation of
the territorial privacy model onto the user level. Privacy awareness is supported by different visualization approaches, which present potential privacy implications to users. Furthermore, the interface supports users in controlling UbiComp systems according to their individual privacy needs, either via direct control options or by defining individual privacy preferences. The user interface was evaluated in a comprehensive scenario-driven user study with several functional prototypes of typical UbiComp systems. The results show that the territorial privacy concept is accepted and that the developed user interface can effectively support users with privacy awareness and control in UbiComp.

**ZUSAMMENFASSUNG**


Diese Arbeit adressiert die beschriebene Problematik der Privatsphäre durch die Entwicklung eines Frameworks für die benutzerzentrierte Unterstützung der Wahrnehmung und Kontrolle von Privatsphäre in UbiComp. Um den Herausforderungen für die Privatsphäre durch UbiComp gerecht zu werden, wurde in dieser Arbeit das Konzept der **Territorial Privacy** definiert. Dieses erweitert die in der Forschung dominierende informationszentrierte Sichtweise von Privatsphäre um physische Aspekte. Territorial Privacy umfasst somit nicht nur Observations, die die Privatsphäre eines Benutzers durch das Erfassen persönlicher Informationen beeinflussen, sondern auch Disturbances, die die Privatsphäre durch ungewünschte Interaktionen oder Eingriffe in die Umgebung eines Benutzers beeinflussen können.


# Discovery & Enforcement Modules

8.1 Privacy Engine ............................................... 164
  8.1.1 Privacy graph instantiation and adaptation ... 164
  8.1.2 Strategy selection for privacy enforcement ... 165
  8.1.3 Exception handling ................................. 165
  8.1.4 Implementation ..................................... 166
  8.1.5 Discussion ............................................ 167

8.2 Personal Device Module ................................. 168
  8.2.1 Registration of devices and observable items .. 168
  8.2.2 Local application framework .................... 170
  8.2.3 Implementation ..................................... 170
  8.2.4 Discussion ............................................ 172
  8.2.5 Related work ......................................... 172

8.3 Trusted Environment Module .......................... 173
  8.3.1 Trust in UbiComp ................................. 174
  8.3.2 ATRACO trusted system ......................... 176
  8.3.3 Privacy management ............................... 179
  8.3.4 Evaluation ........................................... 183
  8.3.5 Discussion ............................................ 185
  8.3.6 Related work ......................................... 186

8.4 Beacon-based Discovery Module .................... 186
  8.4.1 PriFi beacons ........................................ 187
  8.4.2 Implementation ..................................... 189
  8.4.3 Discussion ............................................ 191
  8.4.4 Related work ......................................... 192

8.5 Community-based Discovery Module ............... 192
  8.5.1 Discovery of public video cameras ............. 194
  8.5.2 Evaluation ........................................... 196
  8.5.3 Discussion ............................................ 201
  8.5.4 Related work ......................................... 202

8.6 Privacy Signaling Module ............................ 202
  8.6.1 Disturbances in everyday life ................... 204
  8.6.2 Signaling privacy preferences .................. 208
  8.6.3 Dynamic settings adaptation .................... 211
  8.6.4 Usability study ..................................... 212
  8.6.5 Field trial ........................................... 213
  8.6.6 Discussion ............................................ 217
  8.6.7 Related work ......................................... 219

8.7 Summary .................................................. 220

# User-Centered Privacy Management

9.1 Related Work ............................................. 223
  9.1.1 User interfaces for online privacy ............ 223
  9.1.2 User interfaces for mobile device privacy ... 226
  9.1.3 User interfaces for UbiComp privacy .......... 227
  9.1.4 Security related user interfaces ............... 228
  9.1.5 Summary ............................................. 229
9.2 Design Challenges and Requirements
  9.2.1 Providing awareness
  9.2.2 Providing control
9.3 Design Process
  9.3.1 Initial mockups
  9.3.2 User study: table view and block view
  9.3.3 User study: smartphone-optimized table view
  9.3.4 User study: privacy profile interface
  9.3.5 Discussion
9.4 The PriVis App
  9.4.1 Overview
  9.4.2 Supporting privacy awareness
  9.4.3 Supporting privacy control
  9.4.4 Implementation
9.5 Evaluation
  9.5.1 Functional prototypes of UbiComp technologies
  9.5.2 Methodology
  9.5.3 Participants
  9.5.4 Results
  9.5.5 Discussion
  9.5.6 Design implications
9.6 Summary
10 SUMMARY
  10.1 Contributions
  10.2 Outlook

ACKNOWLEDGMENTS

III APPENDIX
A MODEL APPLICATIONS
  A.1 Model Application to the Running Use Case
  A.2 Model Application to the Working Use Case
B CHANNEL POLICY EXAMPLE
C PRIVIS APP SCREENSHOTS

BIBLIOGRAPHY
  PUBLICATIONS BY THE AUTHOR
  REFERENCES
**LIST OF FIGURES**

<p>| Figure 1.1 | Main contributions of the thesis | 5 |
| Figure 2.1 | Sensing dimensions in UbiComp | 17 |
| Figure 3.1 | Privacy guidelines and principles in UbiComp | 41 |
| Figure 3.2 | Main privacy implications in UbiComp | 49 |
| Figure 3.3 | Presence data showing WhatsApp activity | 57 |
| Figure 3.4 | Conversation probabilities for P10 | 59 |
| Figure 3.5 | Existing privacy-enhancing technologies | 62 |
| Figure 4.1 | Frequencies of awareness and control ratings | 91 |
| Figure 4.2 | Privacy-implication sketches of a sensor band | 95 |
| Figure 4.3 | Factors influencing awareness and control | 98 |
| Figure 5.1 | Overview of the privacy framework | 101 |
| Figure 5.2 | Different types of environments | 102 |
| Figure 5.3 | Example of boundary and territory types | 104 |
| Figure 5.4 | Forms of observations and disturbances | 106 |
| Figure 5.5 | Entities of the running use case | 112 |
| Figure 5.6 | Private territory in the working use case | 114 |
| Figure 5.7 | Private territory in the coming home use case | 116 |
| Figure 6.1 | Instance of the territorial privacy model | 120 |
| Figure 6.2 | Different types of control points | 122 |
| Figure 6.3 | Modeling dependencies between entities | 123 |
| Figure 6.4 | Representation levels of channels | 124 |
| Figure 6.5 | Modeling uncertainties of privacy implications | 126 |
| Figure 6.6 | Disabling an entity with control points | 133 |
| Figure 6.7 | Enforcing desired entities and channels | 134 |
| Figure 6.8 | Enforcing undesired entities and channels | 136 |
| Figure 6.9 | Enforcing desired and undesired sets | 136 |
| Figure 6.10 | Model instance of the coming home use case | 137 |
| Figure 7.1 | Discovery strategies for policy collection | 141 |
| Figure 7.2 | High-level structure of a channel policy | 146 |
| Figure 7.3 | Structure of an entity description | 147 |
| Figure 7.4 | Examples of control point specifications | 149 |
| Figure 7.5 | Components of a channel specification | 151 |
| Figure 7.6 | Content description of a channel specification | 152 |
| Figure 7.7 | Content categories of privacy implications | 153 |
| Figure 7.8 | Main structure of a purpose statement | 155 |
| Figure 7.9 | Example of a control point interface | 159 |
| Figure 7.10 | Channel policies with purpose statements | 160 |</p>
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Overview of the privacy agent</td>
<td>163</td>
</tr>
<tr>
<td>8.2</td>
<td>Integration of the privacy engine</td>
<td>166</td>
</tr>
<tr>
<td>8.3</td>
<td>The personal device module</td>
<td>168</td>
</tr>
<tr>
<td>8.4</td>
<td>The trusted environment module</td>
<td>174</td>
</tr>
<tr>
<td>8.5</td>
<td>Ontology of trust groups and access policies</td>
<td>178</td>
</tr>
<tr>
<td>8.6</td>
<td>Trust group management in ATRACO</td>
<td>179</td>
</tr>
<tr>
<td>8.7</td>
<td>Access and privacy management in ATRACO</td>
<td>181</td>
</tr>
<tr>
<td>8.8</td>
<td>Example of a privacy policy ontology</td>
<td>182</td>
</tr>
<tr>
<td>8.9</td>
<td>ATRACO study setup in the iSpace</td>
<td>183</td>
</tr>
<tr>
<td>8.10</td>
<td>Dynamic privacy-aware slideshow adaptation</td>
<td>184</td>
</tr>
<tr>
<td>8.11</td>
<td>The beacon-based discovery module</td>
<td>187</td>
</tr>
<tr>
<td>8.12</td>
<td>Embedding channel policies in WiFi beacons</td>
<td>188</td>
</tr>
<tr>
<td>8.13</td>
<td>Specifying a camera’s affected area</td>
<td>190</td>
</tr>
<tr>
<td>8.14</td>
<td>Preliminary privacy interfaces</td>
<td>191</td>
</tr>
<tr>
<td>8.15</td>
<td>The community-based discovery module</td>
<td>193</td>
</tr>
<tr>
<td>8.16</td>
<td>Main menu and map view of the CSVP app</td>
<td>195</td>
</tr>
<tr>
<td>8.17</td>
<td>Camera details presented in the CSVP app</td>
<td>196</td>
</tr>
<tr>
<td>8.18</td>
<td>Path with cameras in the field trial</td>
<td>197</td>
</tr>
<tr>
<td>8.19</td>
<td>Video cameras on the field trial path</td>
<td>197</td>
</tr>
<tr>
<td>8.20</td>
<td>Awareness results of video cameras</td>
<td>198</td>
</tr>
<tr>
<td>8.21</td>
<td>Relevance of different camera information</td>
<td>199</td>
</tr>
<tr>
<td>8.22</td>
<td>ASQ results for camera registration</td>
<td>199</td>
</tr>
<tr>
<td>8.23</td>
<td>Accuracy results of registered cameras</td>
<td>200</td>
</tr>
<tr>
<td>8.24</td>
<td>The privacy signaling module</td>
<td>203</td>
</tr>
<tr>
<td>8.25</td>
<td>Common sources of everyday disturbances</td>
<td>205</td>
</tr>
<tr>
<td>8.26</td>
<td>Strategies to reduce disturbances</td>
<td>207</td>
</tr>
<tr>
<td>8.27</td>
<td>Screenshots of the PriPref Broadcaster</td>
<td>209</td>
</tr>
<tr>
<td>8.28</td>
<td>Usability results of the PriPref Broadcaster</td>
<td>213</td>
</tr>
<tr>
<td>8.29</td>
<td>Preference distribution of the field trial</td>
<td>215</td>
</tr>
<tr>
<td>8.30</td>
<td>Common profiles created during the field trial</td>
<td>217</td>
</tr>
<tr>
<td>8.31</td>
<td>Sketch of a privacy display in public transport</td>
<td>218</td>
</tr>
<tr>
<td>8.32</td>
<td>Overview of discovery &amp; enforcement modules</td>
<td>221</td>
</tr>
<tr>
<td>9.1</td>
<td>Mockup of radial privacy awareness</td>
<td>233</td>
</tr>
<tr>
<td>9.2</td>
<td>First mockup of table awareness view</td>
<td>234</td>
</tr>
<tr>
<td>9.3</td>
<td>Mockup of revised table awareness view</td>
<td>235</td>
</tr>
<tr>
<td>9.4</td>
<td>Mockup of alternative table awareness view</td>
<td>236</td>
</tr>
<tr>
<td>9.5</td>
<td>Mockup of block-based awareness view</td>
<td>237</td>
</tr>
<tr>
<td>9.6</td>
<td>Relevance of controlling privacy implications</td>
<td>238</td>
</tr>
<tr>
<td>9.7</td>
<td>Utility of profile specification features</td>
<td>239</td>
</tr>
<tr>
<td>9.8</td>
<td>Utility of context-aware profiles</td>
<td>240</td>
</tr>
<tr>
<td>9.9</td>
<td>Mockup of profile management interface</td>
<td>241</td>
</tr>
<tr>
<td>9.10</td>
<td>Tablet with preliminary awareness interfaces</td>
<td>242</td>
</tr>
<tr>
<td>9.11</td>
<td>Task results of table and block view</td>
<td>244</td>
</tr>
<tr>
<td>9.12</td>
<td>Textual conditions in awareness views</td>
<td>245</td>
</tr>
<tr>
<td>9.13</td>
<td>Usability results of table and block view</td>
<td>245</td>
</tr>
</tbody>
</table>
Figure 9.14  Intention to use table and block view . . . . . . . 246
Figure 9.15  Relevance of different visualization aspects . . 247
Figure 9.16  Usability of alternative table view . . . . . . . 249
Figure 9.17  Usability of profile management view . . . . . 251
Figure 9.18  Task results of profile management view . . . . 252
Figure 9.19  Main views of the PriVis app . . . . . . . . . . . 255
Figure 9.20  PriVis app: dependency views . . . . . . . . . . . 256
Figure 9.21  PriVis app: popup dialogs in dependency view 257
Figure 9.22  PriVis app: detail view and filters . . . . . . . . . 258
Figure 9.23  PriVis app: dialogs for direct control . . . . . . . 259
Figure 9.24  PriVis app: privacy profile management . . . . 260
Figure 9.25  PriVis app: menu for profile creation . . . . . . 260
Figure 9.26  Integration of the user interfaces . . . . . . . . . 261
Figure 9.27  Setup of user study with UbiComp systems . . 263
Figure 9.28  Sensor wrist band and health app . . . . . . . . . 263
Figure 9.29  Screenshots of fitness and health app . . . . . . 264
Figure 9.30  Prototype of the door unlock system . . . . . . . 265
Figure 9.31  Prototype of the activity support system . . . . . 266
Figure 9.32  Participants’ technical affinity and attitudes . . 271
Figure 9.33  Results: task completion time . . . . . . . . . . . 273
Figure 9.34  Results: task correctness . . . . . . . . . . . . . 274
Figure 9.35  Results: perceived usability of PriVis app . . . . 280
Figure 9.36  Results: perceived usefulness of PriVis app . . 281
Figure 9.37  Results: perceived privacy concerns . . . . . . . 286
Figure 9.38  Results: perceived privacy awareness . . . . . . 287
Figure 9.39  Results: perceived privacy control . . . . . . . . 287
Figure 9.40  Results: perceived usefulness of systems . . . . 288
Figure 9.41  Results: intention to use systems . . . . . . . . . 288
Figure A.1  Model instance for the running use case . . . . . 309
Figure A.2  Model instance for the working use case . . . . . 311
Figure C.1  PriVis app screenshots of task 2a . . . . . . . . . 319
Figure C.2  PriVis app screenshots of task 2b . . . . . . . . . 320
Figure C.3  PriVis app screenshots of task 2c . . . . . . . . . 320
Figure C.4  PriVis app screenshots of task 2d . . . . . . . . . 321
Figure C.5  PriVis app screenshots of task 3a . . . . . . . . . 321
Figure C.6  PriVis app screenshots of task 3b . . . . . . . . . 322
Figure C.7  PriVis app screenshots of task 3c . . . . . . . . . 322
Figure C.8  PriVis app screenshots of task 3d . . . . . . . . . 323
Figure C.9  PriVis app screenshots of task 4a and 4b . . . . 323
Figure C.10 PriVis app screenshots of task 4c . . . . . . . . . . 324
Figure C.11 PriVis app screenshots of task 4d . . . . . . . . . . 324
LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Distribution of mDNS device names</td>
<td>55</td>
</tr>
<tr>
<td>4.1</td>
<td>Main factors influencing privacy awareness and control of location privacy</td>
<td>75</td>
</tr>
<tr>
<td>4.2</td>
<td>Main factors influencing privacy awareness and control on mobile devices</td>
<td>79</td>
</tr>
<tr>
<td>4.3</td>
<td>Main factors influencing privacy awareness and control in video and recording systems</td>
<td>81</td>
</tr>
<tr>
<td>4.4</td>
<td>Main factors influencing privacy awareness and control in smart homes and AAL</td>
<td>85</td>
</tr>
<tr>
<td>5.1</td>
<td>Examples of different observer types</td>
<td>108</td>
</tr>
<tr>
<td>5.2</td>
<td>Examples of different disturber types</td>
<td>109</td>
</tr>
<tr>
<td>5.3</td>
<td>Entities of the running use case</td>
<td>113</td>
</tr>
<tr>
<td>5.4</td>
<td>Privacy implications of the running use case</td>
<td>113</td>
</tr>
<tr>
<td>5.5</td>
<td>Entities of the working use case</td>
<td>115</td>
</tr>
<tr>
<td>5.6</td>
<td>Privacy implications of the working use case</td>
<td>115</td>
</tr>
<tr>
<td>5.7</td>
<td>Entities of the coming home use case</td>
<td>117</td>
</tr>
<tr>
<td>5.8</td>
<td>Privacy implications of the home use case</td>
<td>117</td>
</tr>
<tr>
<td>6.1</td>
<td>Purpose properties of involved entities</td>
<td>121</td>
</tr>
<tr>
<td>6.2</td>
<td>Properties in the coming home use case</td>
<td>138</td>
</tr>
<tr>
<td>7.1</td>
<td>Possible actions of a purpose statement</td>
<td>156</td>
</tr>
<tr>
<td>8.1</td>
<td>Performance results of the privacy engine</td>
<td>167</td>
</tr>
<tr>
<td>8.2</td>
<td>Performance results of privacy enforcement</td>
<td>171</td>
</tr>
<tr>
<td>9.1</td>
<td>Overview of study tasks</td>
<td>270</td>
</tr>
<tr>
<td>9.2</td>
<td>Correlations of privacy and usefulness factors</td>
<td>289</td>
</tr>
<tr>
<td>A.1</td>
<td>Properties in the running use case</td>
<td>310</td>
</tr>
<tr>
<td>A.2</td>
<td>Properties in the working use case</td>
<td>311</td>
</tr>
</tbody>
</table>
1

INTRODUCTION

1.1 MOTIVATION

Our everyday life is more than ever influenced by computing technologies. The technological advances of the last decades and the decreased costs of hardware make it affordable to equip everyday objects with computing and communication capabilities. While some years ago, a personal computer was the only way to access the Internet, today we see TVs, cars, or even ovens and fridges [89] being online. Furthermore, with the increasing prevalence of smartphones and wireless communication technologies, being online on-the-go has become the new norm. The smartness of those phones is primarily based on their diverse sensing capabilities, which allow to gather information about a user’s context, such as the current location, orientation, or motion. Together with specialized services, users can be supported in everyday activities, e.g., in finding restaurant recommendations or staying in touch with friends.

This shift from personal to mobile computing reflects the first step towards the following envisioned computing era of ubiquitous computing (UbiComp). In contrast to the mostly explicit support by today’s smartphones, in the vision UbiComp, users will be implicitly and unobtrusively supported in their daily activities by numerous invisible devices embedded in their environments. Popular application domains of UbiComp research are smart homes [240], ambient assisted living (AAL) [186], a special form of smart homes for the elderly, and smart user assistants based on mobile and wearable devices [627]. UbiComp systems of those application domains could, for instance, support users in cooking [532], finding lost objects [18], monitoring health conditions [501], or even in relaxation activities by a system’s individual adaptation to a user’s preferences [295].

In order to allow such individual support and adaptation, UbiComp systems typically require several information, e.g., data gathered from different sensors, user preferences, or additional user information. Furthermore, systems often require the ability to interact with users and to intervene in their physical environment, e.g., by automatically opening doors, controlling blinds of a room, playing music, or providing information on ambient displays [599].

While those new technological advances often provide more convenience, more efficiency, and often enable new promising application domains, they do not come without drawbacks. Especially the protection of users’ privacy when using those technologies is a challenging
but highly relevant topic. When talking about privacy today, most people think of information privacy, i.e., the protection of their personal and sensitive information. There is no doubt that information privacy is one of the most dominant privacy factors, especially in the context of the online world. However, privacy is more than protecting personal information. From a traditional point of view, privacy can be regarded as the “right to be left alone” [681] or a “state in which one is not observed or disturbed by other people” [480].

Even today without UbiComp, people encounter challenges when protecting their everyday privacy in terms of information privacy, but also in terms of the right to be left alone and to be free from disturbances. Increasing numbers of people use a plurality of computing devices, produce considerable amounts of information, and exchange it with a multitude of different persons or organizations, which makes it increasingly challenging to keep control over their information. Furthermore, mobile devices provide people with permanent availability for incoming phone calls, messages, or notifications. Devices are beeping or blinking, for instance, when their batteries are running low, when coffee machines remind users that they want to get decalcified, or when cars warn users that they drive too fast. Other systems might autonomously intervene in a user’s environment, for instance, automatic blinds that adapt to the current light conditions, or autonomous cleaning robots. Accordingly, the general question arises, if it is still possible for people to be in a state in which they are truly unobserved and undisturbed by technology?

Many people share their lives on online social networks such as Facebook or report their activities on micro blogging platforms such as Twitter. However, in recent years companies such as Facebook, Google, or Apple made negative headlines regarding information privacy issues. Facebook was repeatedly criticized for its too open default privacy settings [598], which often lead to a mismatch between privacy expectations of users and real exposure of their Facebook profiles [415]. Not being aware of potential information leaks can have severe privacy implications, as shown by “Girls Around Me” [670], “Please Rob Me” [106], and similar stalking applications, which allow tracking the location of users and aggregating publicly available information about them from different online services [41]. Apple was criticized for storing logs of location information, which allowed to reconstruct complete movement profiles of users [418]. Similar location privacy issues attracted considerable attention regarding stored connection information of mobile phone providers in Germany. The politician Malte Spitz showed how the logged information about his mobile phone connections could be used to reconstruct his movements over a time period of six months [94]. Google was criticized for applying a unified but too generic privacy policy to all of its services, which lacks transparency about the detailed data handling
practices [54]. Also the Google Glass project raised privacy concerns and already led to it being banned from different venues like bars or restaurants [140]. However, Google recently conceded to revise its privacy policies in order to ensure compliance with European data protection regulations [688], and there are also ongoing efforts of the Federal Trade Commission (FTC), which already have positively influenced the data handling practices of large companies in the US [302].

The increased discussions of privacy affairs in news and politics underline the potential influence of technological advances on our privacy and existing privacy concerns among users. The rise of Ubicomp will further intensify privacy issues caused by technology as systems will become more and more integrated into our environments. A prominent example of existing privacy-affecting technology is closed-circuit television (CCTV) surveillance. The deployment of surveillance cameras has rapidly increased during the last years. For instance, in the UK there is roughly one camera for every 32 citizens [405], making UK the world-leading surveillance society according to Privacy International’s privacy ranking of 2007 [524]. The large number of surveillance cameras makes it difficult to handle the huge amount of video streams by the relatively small number of security personnel. The unconventional UK Internet Eyes project [586] tried to solve this issue by opening camera surveillance to the public. The project claims that everyone should be able to help in catching criminals. But who could guarantee that this access will not be misused? In Germany, the number of installed surveillance cameras has increased as well [341], which caused numerous complaints about inappropriate surveillance in different parts of Germany [340, 117] and has also led to a protest movement aiming to destroy as many surveillance cameras as possible [623]. The widespread deployment of this surveillance technology could even mean that you will be surveilled in remote areas, e.g., when taking a walk in the woods [42]. Recent developments also suggest the use of robots and drones as surveillance tools, e.g., to replace night watchmen [597, 434].

The issue becomes even worse when surveillance systems are combined with facial recognition technologies [566], allowing for autonomous identification of people in larger crowds, or even inference of their heart rate from video footage [698]. In most cases, observed persons will not be aware of installed surveillance systems and especially of involved scanning technologies, leading to a mismatch of perceived and real privacy implications. This power imbalance due to asymmetric knowledge is a particular problem of Ubicomp systems, because they aspire to be an invisible part of our environment. In many situations, users will not even be aware that those systems exist, until an explicit interaction or operation occurs. And even if users are aware of their existence, they might not be fully aware of how such systems could affect their privacy.
The smarter those systems become, the more difficult it will be for users to understand their actual privacy implications. The rise of upcoming smart technologies underpins this problem. For instance, today’s smart TVs allow vendors and providers to record users’ watching behavior [347, 267] or even their voice [348], and smart meters allow suppliers to infer performed activities of users in their homes [549, 458]. Private activities such as showering or using the toilet could even be observed by fingerprinting approaches based on transmissions from wireless home sensors [620]. In London, smart recycling bins have caused privacy debates, because they tracked the MAC addresses of WiFi-enabled smartphones of passers-by [178].

This all comes down to a fundamental dichotomy of UbiComp technologies. On the one hand, the smartness of such technology has the power to enhance and support our lives. On the other hand, this smartness combined with the invisible nature of UbiComp challenges our privacy. Users will often not be aware of a system’s privacy implications, or even of the system’s presence. Potential privacy implications can be wide ranging due to systems’ diverse sensing, processing, and acting capabilities. Furthermore, the inter-connectivity of UbiComp systems results in physical boundaries losing their ability to demarcate and protect a user’s privacy. Because information flow is not stopped by walls or doors, communication technology replaces physical boundaries with virtual ones, which are not perceivable by users. This lack of awareness may lead to discomfort and a feeling that privacy expectations are violated when users discover later on that they have been observed by a system, or that a system operated unexpectedly. The same effect could be caused by undesired interventions in the user’s environment or by undesired interactions with the user. Only if users are aware of potential privacy implications can they decide whether to use a system or decide what steps to take in order to control their privacy.

Therefore, the fundamental research questions of this work are: How can we support users in gaining awareness of potential privacy implications stemming from UbiComp systems? And how can we give users back the control of their privacy and enable them to enforce their individual privacy preferences in such systems? These research questions and related contributions of this thesis are discussed in the following.

1.2 Research Questions & Contributions

The primary research goal of this thesis is the contribution of a user-centered framework for supporting individual users with privacy awareness and control in UbiComp environments. In contrast to most previous work, our\(^1\) notion of privacy has not been limited to aspects

\(^{1}\)Following the common convention in Computer Science literature, the first person plural will be used to refer to the author throughout this thesis.
of information privacy, but has been extended to also cover physical privacy aspects in our concept of territorial privacy. In this context, the following research questions with related sub-questions have been addressed in this thesis:

R1 How can informational privacy aspects and physical privacy aspects be addressed in a territorial privacy model?
R1.1 What are the main privacy implications stemming from UbiComp systems?
R1.2 What are the aspects of privacy implications users want to be aware of and want to control?
R1.3 How can a territorial privacy model support privacy awareness and control?

R2 How can territorial privacy be realized at the system level?
R2.1 How can the territorial privacy model be initiated at the system level?
R2.2 How can privacy implications be discovered at the system level?
R2.3 How can privacy decision be enforced at the system level?

R3 How can privacy awareness and control effectively be realized at the user level?
R3.1 How can the territorial privacy model be mapped onto the user level?

R3.2 How can users be made aware of complex privacy implications in UbiComp?

R3.3 How can users be supported in controlling UbiComp systems according to their privacy needs?

This thesis addresses these questions by proposing a user-centered approach to support privacy awareness and control in UbiComp. The main contributions cover user-level and system-level aspects which are based on a new model for territorial privacy (see Figure 1.1):

Awareness of Privacy Implications We conducted two studies in which we investigated privacy implications of zero-configuration networking (Section 3.4.2) and mobile messaging applications (Section 3.4.3), two technologies commonly used on mobile devices. Our results show that these prevalent technologies pose several privacy risks, which users are often not aware of. Together with similar findings of related work, our results motivate the need for enhancing privacy awareness in UbiComp.

Privacy Concerns & Human Factors In order to guide the development of our territorial privacy model we conducted an extensive literature review focusing on existing user studies which investigated users’ privacy concerns in the context of UbiComp applications (Chapter 4). We identified essential factors of observations and disturbances that need to be considered in order to effectively provide privacy awareness and control at the user level. We complemented the results of the literature review with further research by conducting an online survey (Section 4.6) and a focus group session (Section 4.7) in which we investigated privacy concerns of elderly persons towards ambient assisted living technologies. Such technologies are one of the major UbiComp applications envisioned. However, elderly persons will likely be the most challenged in coping with such technological changes, especially in terms of privacy awareness and control.

Territorial Privacy Model Based on the results of the literature review and on our definition of territorial privacy, we developed a graph-based territorial privacy model (Chapter 6). The model allows to capture which entities affect a user’s privacy, how and why. Its formalization further allows to infer dependencies between entities, and consequences or conflicts of potential control decisions. The model supports identification of the most efficient control strategies, which enables enforcement of users’ privacy decisions at the system level.
**Model Instantiation & Channel Policies** In order to instantiate the territorial privacy model at the system level we propose the concept of channel policies (Section 7.3). Channel policies provide information on how and why an entity is affecting a user’s privacy with respective observations and disturbances. Furthermore, channel policies provide references to available control points for privacy enforcement.

**Discovery & Enforcement Modules** In order to make channel policies practical, systems must be able to discover them at the system level. We developed five discovery and enforcement modules (Chapter 8) which allow the discovery of channel policies and the enforcement of users’ privacy control decisions, respectively: The personal device module, the trusted environment module, the beacon-based discovery module, the community-based discovery module, and the privacy signaling module. To cope with the heterogeneity of UbiComp systems, with their different privacy implications, and with the different settings and conditions of a user’s environment, different discovery and enforcement mechanisms have been developed that are suitable for certain environments. The modules implement both optimistic and pessimistic approaches, in order to satisfy the different requirements and assumptions. We evaluated the proposed discovery and enforcement modules for their technical feasibility and efficiency. The results show that the developed framework is able to efficiently discover and control privacy implications in UbiComp for different scenarios.

**User-Centered Privacy Management** We developed a user interface for user-centered privacy management in an iterative design process with several user studies and online surveys (Chapter 9). The interface maps an instantiation of the territorial privacy model onto the user level. Privacy awareness is supported by different visualization approaches which present potential privacy implications to users. Furthermore, users are supported in privacy decision making and in controlling systems according to their individual privacy preferences. The user interface was evaluated in a comprehensive scenario-driven user study with several functional prototypes of typical UbiComp systems causing complex privacy implications. The results suggest that our territorial privacy concept and our approach to support privacy awareness and control is highly accepted. The results further show that the developed user interface can effectively support users with privacy awareness and control of complex privacy implications in UbiComp.
Parts of this work have been published in peer-reviewed international conferences and journals. A complete overview of the author’s publications is given on page 325ff. Relevant publications will also be referred to in the respective sections of this thesis.

1.3 THESIS OUTLINE

The following chapters are structured in two main parts. The first part, Background & Problem Analysis provides a discussion of the general vision of UbiComp, its driving key technologies, the current research state of the art, together with the challenges and implications associated with UbiComp in Chapter 2. Chapter 3 introduces privacy, as one of the primary UbiComp challenges, and provides a discussion of different theoretical privacy frameworks and dimensions. It further clarifies the concept of territorial privacy and identifies common privacy implications of UbiComp applications, which are also confirmed by our two studies investigating privacy implications of zero-configuration networking and mobile messaging applications. Chapter 4 provides an extensive literature review of existing user studies related to privacy in UbiComp and presents the results of our own user studies, which investigated privacy concerns of elderly persons towards UbiComp technologies. The results guided the development of our territorial privacy model.

The second part, User-Centered Privacy Awareness & Control, presents the main contributions of this thesis. Chapter 5 provides an overview of the framework together with three representative use cases. Chapter 6 introduces the territorial privacy model and its respective formalization. The structure of channel policies required for the instantiation of the model and the general approach for policy discovery are discussed in Chapter 7. The concepts, development, and evaluation of different discovery and enforcement modules, which provide awareness and control at the system level, are described in Chapter 8. Chapter 9 describes the iterative design process of our user-centered privacy management interface with the results of preliminary user studies and online surveys. It further discusses the evaluation of the resulting user interface in a comprehensive scenario-driven user study with several functional prototypes of UbiComp systems. A summary and discussion of the results and contributions of this work is provided in Chapter 10.
Part I

BACKGROUND & PROBLEM ANALYSIS
The Vision of UbiComp was introduced by Marc Weiser in the early 1990s at Xerox PARC [682]. Weiser argued that the conventional “idea of personal computing is misplaced” because computers require too much attention of users [683]. Rather than bringing tasks to the computer, Weiser envisioned a world in which everyday tasks of users are supported in their physical environment by invisible and “calm” computing technologies, which are indistinguishable from the “fabric of everyday life.” He argues that “only when things disappear in this way are we freed to use them without thinking and so to focus beyond them on new goals.” The main goal of this vision is to support user tasks of everyday life more efficiently and provide users more convenience and safety in their everyday activities.

In his article, Weiser describes a normal day of a fictional person Sal, who is supported in her everyday activities by UbiComp technology. When Sal wakes up, she is asked for coffee and receives information about activities in her neighborhood through an ambient display that also informs her that her children are already awake and in the kitchen. On the way to her office, Sal is warned about traffic jams and guided to the next available parking spots. At work, she virtually shares her office with another colleague. They use several interconnected devices to collaborate and communicate remotely with each other. These scenarios highlight typical application domains and characteristics of Weiser’s UbiComp vision. Similar to these scenarios, UbiComp research often focuses on the development of smart environments, like a smart home or smart office, and smart devices like a smart car. The majority of projects and existing systems is characterized by situation and context awareness, ubiquitous inter-connectivity, and individual user support or smartness.

To realize situation and context awareness, UbiComp systems require different kind of sensors and information sources which contribute to the inference of context. Context in this respect relates to “any information that can be used to characterize 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 applications themselves” [191]. According to Dey “a system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user’s task” [191]. The location of a device or a person is one of the most important contextual information mentioned
by Weiser: “If a computer merely knows what room it is in, it can adapt its behavior in significant ways without requiring even a hint of artificial intelligence” [682]. Therefore, research in location systems attracted considerable research since the beginning of UbiComp [301]. But also higher level context information, e.g., a user’s activity, or emotional state, are of importance in order to provide individual user support.

Ubiquitous inter-connectivity depicts another essential characteristic of UbiComp. The power of smartness in UbiComp systems is often based on the interconnection of different distributed devices, systems, and services. In a smart home environment, embedded devices, like sensors or actuators, typically are connected to a central processing component, which controls different actuators based on gathered and combined information from different sensors. Such smart home infrastructures can further be connected with external online services, or even be connected with other smart environments, in order to support users beyond physical boundaries. In a perfect UbiComp world all available systems would be interconnected in order to provide the best user support. As Weiser stated: “Already computers in light switches, thermostats, stereos and ovens help to activate the world. These machines and more will be interconnected in a ubiquitous network” [682].

The realization of individual user support or smartness primarily depends on the two previously discussed characteristics. The more a UbiComp system knows about a user’s current situation, the better it can support individual user needs. Individual support can be wide-ranging from providing information via audiovisual output, controlling devices based on implicit user input, or autonomously adapting the user’s environment based on contextual information. In Weiser’s lab it was even at this early stage of UbiComp research possible that rooms greet people by name, telephone calls were automatically forwarded to a recipient’s location, receptionists knew where people were, and appointment diaries wrote themselves [682].

The term ubiquitous computing and its involved visionary goals are also reflected in the related terms pervasive computing, ambient intelligence, and the internet of things. Pervasive computing was usually associated with a more pragmatic view on realizing similar goals as in Weiser’s UbiComp vision, but with already existing technologies. Thus, even though the term was typically used in industry-related contexts, it refers to the same concepts and today is often used interchangeably [565, 558]. For instance, Saha and Mukherjee [558] state that “pervasive computing is about making our lives simpler through digital environments that are sensitive, adaptive, and responsive to human needs.”

Similarly, the term ambient intelligence was introduced by the European Union’s Information Society Technologies Program Advisory Group (ISTAG) to describe the combination of ubiquitous computing, ubiquitous communication, and “intelligent user-friendly interfaces” [687].
The internet of things (IoT) is another term often related to UbiComp [58]. It refers to the inter-connection of everyday objects, which is also reflected in Weiser’s early vision: “When almost every object either contains a computer [. . .], obtaining information will be trivial” [682]. The term itself was first used by Kevin Ashton in 1999 [56] and primarily refers to the interaction between objects in order to offer better efficiency and accountability to businesses in their supply chains, especially without the need of human involvement. The RFID technology to tag, identify, and track objects wirelessly, is often seen as a prerequisite for the IoT [56]. Even if the involved technologies and characteristics of IoT are very similar to those of UbiComp, the biggest difference is the lack of user involvement, where in contrast UbiComp in particular focuses on user involvement and support.

2.2 KEY TECHNOLOGIES & RESEARCH STATE-OF-THE-ART

UbiComp has for many years influenced a broad multidisciplinary research field. The main reason for this is the ultimate goal of UbiComp to solve problems of the real world in application domains such as education, health, assisted living, or sustainability [26].

“The research method for ubiquitous computing is standard experimental computer science: the construction of working prototypes of the necessary infrastructure in sufficient quantity to debug the viability of the systems in everyday use [. . .]. This is an important step towards insuring that our infrastructure research is robust and scalable in the face of the details of the real world.” – Weiser ’93 [683]

This ambitious goal often requires the collaboration of researchers of many different fields, e.g., embedded systems, sensing technologies, artificial intelligence, distributed systems, human computer interaction, medical science, and social science, to name only a few. Since its beginning, UbiComp has found its way on the research agenda of most developed nations [241] and during the last decade has become a prevalent research topic. Today, UbiComp “is no longer a niche research topic, but is best seen as the intellectual domain of all of computing,” as claimed by Abowd [26].

While UbiComp research covers a wide range of technological areas, Weiser’s identified key technologies of a UbiComp system still fit the most applications today [682]: “cheap, low-power computers [. . .], a network that ties them all together, and software systems implementing ubiquitous applications.” Thus, on the one hand, the interplay of different hardware components is required in order to gather, communicate, and process information, and in order to provide user-dependent interaction or adaptation. On the other hand, software components are required that provide abstraction layers for underlying hardware
components and communication technologies in order to support realization of different UbiComp applications.

The following sections will introduce UbiComp key technologies and provide an overview of the research state-of-the-art in middleware for UbiComp applications, sensing technologies, as well as technologies for automation and interaction.

2.2.1 Cheap and low-power computers

According to Weiser’s vision, we will have “hundreds of computers per room,” thus cheap and low-power computers are an essential requirement to deploy large scale UbiComp systems and equip everyday objects with sensing, actuating and processing capabilities. Those capabilities of today’s available hardware components are strongly related to the popular observation of processing power development: Moore’s Law [463]. According to Moore’s prediction from 1965, the power of microprocessors will double every 18 to 24 months.

This rapid development in computational capacity allows to build embedded systems of low cost and small size with processing power that was not available even for the largest desktop computers twenty years ago. Today, we see high-end smartphones [692] with multi-core processors that are equipped with a bunch of sensors and actuators. Typically all smartphones on the market have GPS-sensors, cameras, accelerometers, vibration motors, and speakers on board. While smartphones represent the upper bound of feasible technological features combined in a small handheld device, they typically are not very cheap and require recharging every one or two days. Cheaper and more energy-efficient embedded systems mostly provide lower processing power, less sensing or actuating capabilities, and, in contrast to smartphones, support only specific purposes. Those systems better fit Weiser’s vision to build everyday smart objects, e.g., smart lamps [518], smart wristbands [231], or smart door locks [59], which are already available today.

2.2.2 Communication technologies

Weiser’s second requirement, “a network that ties them all together,” underpins the relevance of communication technologies for UbiComp systems [682]. Even if it is possible to build isolated smart systems, the real benefit of the UbiComp vision relies on the communication and inter-connectivity of different devices and components. Smart everyday objects become even smarter when they can communicate with other objects, for instance to collect and aggregate information from different sources in order to enhance their knowledge base. Especially wireless communication supports this requirement very well, because it enables ubiquitous connectivity. Today there are several
wireless communication technologies for different purposes, mostly depending on the required bandwidth, transmission range, and energy consumption. Similar to Moore’s law, Nielsen [479] formulated a prediction for communication bandwidth in 1998, stating that also bandwidth will roughly double every year. Looking at the bandwidth of available communication technologies today, this prediction again has proven to be quite accurate. For instance, the IEEE 802.11ac [316] standard enables data rates for wireless local area networks of up to 6.9 Gbit/s by combining 256QAM modulation and multiple input multiple output (MIMO) with up to eight spatial streams. With similar techniques, the 4G LTE-Advanced standard [251] provides data rates of up to 1 Gbit/s for long range mobile communications.

For use cases in which short distance communication is sufficient and energy efficiency is the more crucial aspect, communication technologies like near field communication (NFC) [475], Bluetooth low energy (LE) [103], or ZigBee [710] are more appropriate state-of-the-art candidates. Especially Bluetooth LE has been adopted by many vendors to inter-connect personal wearable devices, e.g., to connect a smartphone with heart rate sensors [672], smart watches [510], wrist bands [231], or even smart shoes [366]. An overview of further communication technologies for wireless body area networks (WBANs) can be found in the surveys of Cao et al. [134] and Chen et al. [146].

Because Bluetooth LE focuses on WBANs, devices still require own power sources. NFC or similar communication technologies based on radio-frequency identification (RFID) [691] can passively communicate over short distance (e.g., several centimeters) without any power supply. In this case, energy for transmission is induced by a reader’s radio signal. Passive NFC or RFID tags are widely used for authentication, payment, or product tracking in logistics [210]. ZigBee is another specification for low-power communication based on the IEEE 802.15.4 standard [314]. It supports routing and is especially suited for larger networks and therefore is often used in wireless sensor networks (WSNs) [146, 703] or home automation systems [255].

In addition to the discussed communication technologies above, many other protocols and standards exist for diverse purposes and application domains. This diversity of heterogeneous communication technologies is one of the obstacles UbiComp system developers have to cope with. A decision between multiple available alternatives could be based on diverse criteria, like cost- or energy-efficiency, reliability, or suitability for an application scenario [39].

### 2.2.3 Middleware for ubiquitous applications

While cheap and low-power computers, as well as promising communication technologies already exist for UbiComp, writing software for
Ubiquitous computing systems often remain challenging, as already predicted by Weiser in 1991 [682].

In order to deal with the heterogeneity of underlying communication technologies, as well as with the diversity of different hardware and software components required for Ubiquitous computing systems, several middleware approaches have been proposed [569, 530] to ease the development of ubiquitous applications. The main goal of middleware for Ubiquitous computing is to "match application-needs to available resources, while ensuring quality and efficiency" [530]. According to Raychoudhury et al. [530], Ubiquitous computing middleware can be classified by three design dimensions: the programming abstractions which provide interfaces for developers, the system architectures which could be either centralized or decentralized, and system services and runtime support as specific implementations to achieve the provided abstractions. The core services of most middleware approaches are context management, service management, and reliability support [530].

The goal of context management services is to provide abstractions for context acquisition, context storage, context modeling, and context reasoning in order to encapsulate the process of collecting data from different physical, logical, or virtual sensors [69] and the inference of higher level context information by analysis and aggregation techniques [360]. Knappmeyer et al. [360] and Bellavista et al. [85] provide comprehensive overviews of the current research state-of-the-art in context provisioning middleware for Ubiquitous computing.

Service management aims to provide abstractions for discovery, composition, and access of any hardware or software functionality of a device or component that can be utilized by other devices or components [530]. Different service discovery protocols have been proposed to deal with the heterogeneity and dynamics of Ubiquitous computing systems. A good overview of available discovery mechanisms for Ubiquitous computing can be found in the surveys of Zhu et al. [707], Edwards [206], and Seno et al. [585]. Prominent candidates used by industry are the Simple Service Discovery Protocol (SSDP) of Universal Plug and Play (UPnP) [660], Apple’s Bonjour protocol [52], or the Service Discovery Protocol (SDP) of Bluetooth [103]. Service composition refers to the process of combining discovered service components to logical higher-level services [119, 625, 530].

In order to support reliability of a Ubiquitous computing system, different middleware solutions have been proposed to provide fault-tolerance to context and service management. Proposed solutions for context management are context preprocessing and context inconsistency detection and resolution [530]. Realizing fault-tolerance for service management requires the adaptation to dynamic and unpredictable changes, which is especially important for the composition of services. Dynamic service composition approaches have been proposed which support re-planning of the composed service during runtime [119, 457, 398, 662].
2.2.4 Sensing technologies

Gathering information about users (user-centric sensing) and about their environments (environment-centric sensing) depicts one of the most important requirements of UbiComp systems in order to provide context-based adaptation and support. Context information can be collected by different physical, virtual, or logical sensors [318, 360]. Physical sensors gather raw real-world data. Examples of such sensors are video cameras, motion sensors, or GPS sensors. They are the main sources for inferring situations and context. Inference is further supported by virtual sensors, which refer to information sources of the virtual world, e.g., calendar entries, database entries, or user profiles. Finally, logical sensors typically provide higher-level information that is based on the composition of different physical and virtual sensors. For example, inferring a user’s activity by combing a calendar entry, the current position, and motion patterns.

Sensing technologies can further be deployed on users’ personal devices (user-based sensing), or in the environment of users (infrastructure-based sensing). Figure 2.1 depicts these different dimensions and types of UbiComp sensing technologies.

User-centric sensing

At the very beginning of UbiComp research, user-centric sensing technologies mostly focused on realizing identification and localization of users [675, 683]. Today, the use of RFID technology is a common approach to identify, locate, and track objects as well as people. This approach is often utilized in retail and health-care applications [699, 708]. While identification of people based on RFID requires users to carry an RFID-enabled device or tag, other identification approaches aim at relying on individual characteristics of a person gathered by different sensor technologies. Popular approaches are identification systems based on physiological biometrics, like the recognition of a person’s face [322, 408], fingerprint or iris [327]. But also speech recognition or facial temperature analysis via infrared sensors are
already feasible identification approaches [326]. Other biometric approaches use a person’s gait, i.e., the way a person walks, for identification via silhouette-based recognition [673, 483], recognition with floor sensors [456], or recognition with wearable motion sensors [335]. Kwapisz et al. [375] have demonstrated that gait-based identification is even feasible with conventional acceleration sensors of smartphones. Novel identification methods based on behavioral biometrics leverage the uniqueness of observed skills, preferences, or strategies of people while performing everyday tasks [702] such as keystroke dynamics [72], touch screen patterns [182], credit card use [113], or even the car driving style [217, 497].

Identification technologies are often used in combination with localization [318]. While GPS has been the standard localization technology for outdoor scenarios, indoor localization still remains a challenging topic. Many different localization approaches have been proposed for UbiComp and particularly indoor scenarios [301, 413, 277, 442]. Indoor localization techniques in general can be categorized into four groups [285]: Lateration and angulation systems, which calculate the position based on the distance or bearings between a device and base stations with known location, e.g., the Ubisense system based on ultra-wideband (UWB) [658]. Proximity-based systems provide location information based on the proximity of a device to known base stations. The positioning accuracy depends on the coverage and range of used base station technologies and can range from several kilometers (e.g., GSM base stations) to several meters (e.g., Bluetooth base station), or even centimeters (e.g., RFID base stations). In radio fingerprint systems locations are prescanned for radio properties, e.g., the signal strength of base stations, in order to create a reference map for later comparisons to real-time scans by a user device. Completely without any infrastructure requirements operate dead-reckoning systems, which utilize user-worn sensors to estimate the position of a user in relation to their previous position [285].

While the identity and location of a person are often the most relevant context information for UbiComp, there is much more information that can be gathered by many different sensing technologies. Today, user-based sensing technologies often focus on mobile phone sensing by utilizing embedded sensors of a user’s smartphone in order to enable personal, group, and community scale sensing applications [387]. Phone sensors can be combined with wearable sensors to gather chemical, thermal, mechanical, or acoustic information from a person’s body [134], e.g., to gather vital parameters, such as, heart rate, blood sugar, or the temperature of a person. The combination of such wearable sensors through a wireless body area network (WBAN) enables many different applications, e.g., health monitoring or activity tracking [387, 146].
A central goal in many sensing applications is the inference of higher level information from low level sensor data, e.g., the inference of a person’s behavior or activity \[393, 387\]. Beside a person’s identity and location, the activity is another essential context factor to enable reliable and effective support by a UbiComp system. Examples for common recognizable activities are locomotion (e.g., walking, running, or cycling), or daily activities (e.g., eating, watching TV, or reading). Both, user-based sensing \[115, 73, 393\], and infrastructure-based sensing approaches \[344, 562, 656\], have been proposed in literature for activity recognition. Infrastructure-based recognition approaches often rely on sensors embedded in real world objects a person interacts with (e.g., washing machine, stove) \[344, 562\] to enable the recognition of complex activities. Other approaches utilize cameras in a user’s environment in order to visually recognize performed activities \[656, 133\]. Those approaches have advanced significantly since the invention of low cost depth cameras, e.g., Microsoft’s Kinect \[455\]. While infrastructure-based approaches often allow to recognize more complex activities (e.g., cooking or showering) than user-based recognition approaches, they typically require the presence and interaction of users, and thus are more suited for smart home or assisted living applications with static infrastructure in a controlled environment.

Wearable sensors, as well as personal device sensors, are on the other hand more suited for environment-independent activity recognition and situations in which simple activities (e.g., walking or sitting) are sufficient. Novel opportunistic activity recognition approaches try to use any kind of available sensors (e.g., wearable or environmental) in order to deal with changes in sensor configurations and to autonomously learn activities with different sensor sets \[545\].

**Environment-centric sensing**

Environment-centric sensing approaches gather information about environmental conditions and changes. In UbiComp systems the context information about the environment is often used in combination with user-centric sensing approaches in order to provide more reliable adaptation and support decisions with respect to a user’s goal. Sensing approaches of this kind are typically infrastructure-based and focus on applications like surveillance \[25\], environmental monitoring, or smart homes, e.g., by deploying a large number of low-power camera nodes \[611\]. Other types of sensors could measure thermal, chemical, or magnetic properties of the environment \[703\]. To ease the deployment of such sensor nodes, combining them in a wireless sensor network (WSN) is a reasonable approach for large scale sensing purposes \[40\]. Typical application domains for such WSNs are monitoring (e.g., outdoor environmental monitoring, or power monitoring) and tracking (e.g., of objects, animals, or vehicles) \[703\].
Thanks to the increasing ubiquity of smartphones and their diversity of embedded sensors, user-based sensing of environmental properties has become a common practice. Leveraging sensors of personal smartphones and combining them into a large scale sensor network can support similar goals like WSNs, but without the need for expensive deployments. This type of sensing is also referred to as participatory sensing [122, 154], opportunistic sensing [132], citizen sensing [107], or urban sensing [173] when focusing on the collection of information about the urban environment. Examples are the collection of information about traffic conditions (as already realized by Google Maps [76]), about noise pollution [528], or about disease distributions (e.g., flu or allergies) [594].

2.2.5 Automation, actuation and interaction

While sensing technologies are necessary to determine the current context of a user or of an environment, it is only beneficial for the user when the system reacts in some way to the determined context. In order to achieve this state of context-awareness, UbiComp systems either need capabilities to interact with users or to automatically execute or adapt services. From an architectural point of view a system’s reaction is implemented on the application layer [69]. However, before an action can be implemented, it requires the whole process of information acquisition, information analysis, as well as decision and action selection [502, 194]. This process is also referred to as the context-aware system cycle [360].

Providing automation based on context reasoning can be applied on different levels. According to Parasuraman’s ten levels of automation [502], the second-highest level when “the computer executes automatically, and informs the human only if it […] decides to,” does fit the UbiComp vision best. Interaction with the user should only be initiated where necessary. While today automation is prevalent in many safety-critical and time-critical applications [503], e.g., aircraft control, or in-car safety systems, it is also more and more relevant for non-critical everyday applications, e.g., in home automation to control entertainment, security, lighting, or air-conditioning systems [286]. Also our smartphones provide some level of automation, e.g., by increasing a display’s brightness based on the environment’s luminosity or by providing us with information about important appointments or the latest news.

In UbiComp, automation may involve the control of actuators in the user’s physical environment, either to adapt the environment (e.g., by controlling light switches or blinds [255, 626]), or to attract a user’s attention for interactions by controlling visual, acoustic, or haptic output devices. Similar to sensors, the miniaturization of microelectronics allows to embed all kind of actuators even in the small-
est everyday objects, e.g., in heated shoes [643] or in vibration-enabled necklaces [559]. Assistance in the home environment can be further enhanced by autonomous robots for many different purposes [626, 81, 589]. Already common are vacuum robots that clean rooms without requiring any user interaction [237]. Research on ubiquitous robotics aims at supporting elderly persons at home [589] and seamlessly augmenting a users environment from the home to the public with different interconnected robots [560].

However, even if Weiser envisioned UbiComp as a calm and invisible technology facilitating implicit interaction [574], explicit human-computer interaction is still an important part of many UbiComp applications but mostly very different to traditional interactions with desktop applications. The interaction itself may remain invisible, but only “to an extent where the person can focus on performing the tasks, albeit mediated by the system, without worrying about the technology itself” [573].

For UbiComp robotics this opened a wide research area of human robot interaction [257, 235, 414]. More generally, research has been conducted to enable interactions in UbiComp through a human’s body, gestures, or even facial expressions and emotions [323, 668]. Also brain-computer interfaces could improve user experience and task performance when combined in a multimodal interaction approach [280]. Ambient output modalities, e.g., public displays [466, 248], personal projected displays [552], or speech dialog systems [294, 283], enable pervasive interaction, everywhere and anytime.

2.3 Applications

The technologies introduced and discussed in the former sections allow the realization of various applications for many different use cases. Common application domains of UbiComp are smart environments at home or at work, and wearable or mobile applications, often with focus on healthcare and assisted living. The following sections provide a short overview of applications from those domains. For a more comprehensive overview, please refer to existing surveys [557, 705, 166, 494, 186], or the latest proceedings of the International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp) [657].

2.3.1 Smart Environments

Smart environments refer to infrastructure-based UbiComp applications which aim at supporting a user’s everyday tasks. Typical application domains are work, education, home, or shopping.

The smart work environment was one of the earliest domains for UbiComp applications, already investigated by Weiser and colleagues at Xerox PARC [683]. Today there are still many research projects aiming to provide more efficient task completions or collaboration. Smart
meeting systems support users in archiving, analyzing, or summarizing meetings to ease and enhance the organization process [705]. Most approaches utilize automatic audio and video recordings for this purpose, but also pen-stroke sensors, motion sensors, or head-tracking sensors are used to determine required context information, such as locations, seat positions, emotions, or whiteboard notes of participants [705]. In non-collaborative office situations where a person seeks the attention of another person, sensors in the environment (e.g., video cameras or microphones) can help to assess the interruptibility of each other, in order to prevent interruption in socially-inappropriate moments [234].

Another popular domain of UbiComp research is the smart home. Existing work aims at supporting everyday activities and provide safety, comfort, and economy [557, 166]. In the last decades, several research projects have build real-world test-beds in form of smart apartments [319, 659, 440] or smart houses [296, 249, 240].

While already many products for home automation are available and more homes are being equipped with home automation technology, there is still a long way to go before commercial home automation will reach the vision of UbiComp. The main reason for this is the lack of adaptability and intelligence of existing systems [635]. Most systems still only adapt to manually programmed tasks, or to simple rule-based sensor readings, e.g., blinds are automatically closed at a specific time, on a specific luminosity, or wind speed. Research tries to enhance intelligence and adaptability in home automation, e.g., by automatically controlling home heating based on sensing and prediction of occupancy in homes [579, 419], or controlling light conditions based on general user preferences [95].

A typical everyday activity that is often addressed by research in smart homes is cooking. Reichel et al. [532] propose an adaptive kitchen system, which supports inexperienced users in cooking even complex dishes. A similar smart kitchen is proposed by Chen et al. to recognize cooking activities and provide real-time nutrition information to support healthy cooking [144]. The Cooktab is a smart cutting board proposed by Sato and Tsukada [564] to allow the automatic recording of recipes from sensed cooking activities. Hooper et al. [308] showed that an instrumented kitchen can even contribute to learning of a foreign language while cooking. Sugiuora et al. [631] propose an autonomous cooking system based on small robots that perform cooking tasks according to a given recipe.

Domestic robots have become more prevalent in recent years and also attracted considerable research interest in the context of smart homes. In addition to cooking and already common cleaning robots, different robots have been proposed for cloth folding [630], object fetching [325] or manipulation tasks, such as open doors or cabinets [619, 324]. There are also great efforts in making robots more
social, e.g., by giving them faces to express human-like emotions [235, 257]. Research on ubiquitous robotics [560] even aims at seamlessly augmenting not only home but any kind of environments with different interconnected ecologies of robots. For example, the combination of home, transportation, and retail robots to allow the delivery of products from the supermarket to the kitchen table [563]. Amazon is currently working on flying drones that could autonomously deliver packages to customers, but are currently inhibited by legal restrictions [666].

Moving from home and work environments into the public, research often focuses on shopping applications in order to provide customers with better shopping experiences or to support retailers with better marketing strategies and more efficient processes in logistics. In Germany, the Metro AG’s Future Store Initiative [451] is one of the leading drivers of new technologies in retail from an industry perspective. New technologies are deployed and analyzed in different real world test-beds. For instance, in the real,- Future Store customers can use a mobile shopping assistant to scan products and pay via finger scan [690]. Smart shopping carts have been the focus of several research projects in order to support users in finding products by macro-navigation in a store [336, 101] or even by micro-navigation in front of a shelf [406]. Kalnikaite et al. [337] provide a clip-on shopping handle that tries nudging people to buy products with lower mean food mileage to counteract global warming. Further research directions are smart mirrors that aim to support users in choosing from different products without the need to try on each of them, e.g., clothes [449] or jewelry [158].

### 2.3.2 Wearable and mobile applications

Wearable and mobile UbiComp applications typically address situations that are more related to body-centric or mobile activities. Several works exist that try to enhance specific tasks in different fields of work by wearable sensors and actuators. For example wearable activity tracking systems to support firefighters in real-world missions [225, 332], or to support maintenance workers in car manufacturing processes [627]. Further research addresses focused assistance for specific sport activities. For instance, facilitating body-worn sensors to support the assessment of running techniques [629], swimming techniques [436], weight lifting exercises [667], or even climbing exercises [380].

With the use of different smartphone sensors, the tracking of sport activities (e.g., running or biking) has already become a common practice among professional but also amateur athletes. Several smartphone apps exist that allow analyzing the monitored activities online or to share them with others [215, 172, 553]. GPS-sensors and
accelerometers of smartphones can be combined with wearable heart rate sensors to monitor vital parameters and provide further statistics about fitness conditions and training development. For walking activities, Sumida et al. [632] have demonstrated that even without a heart rate sensor, it is possible to estimate the heart rate only from acceleration and GPS data.

### 2.3.3 Healthcare and assisted living

Research in UbiComp applications for healthcare is one of the most often addressed application domains reflected by many existing surveys [146, 501, 43, 372, 494, 495, 663]. A very related application domain is presented by assistive systems for elderly with the focus on enhancing safety, well-being, independence, and mobility [186, 626]. This application domain in combination with smart home systems is often referred to as ambient assisted living (AAL) and due to an aging society gained global interest, e.g., in the European Union’s joint research programme on AAL [221], or the more recent European Innovation Partnership on Active and Healthy Aging [222].

Healthcare applications are typically based on sensing one or multiple vital parameters in order to monitor health conditions, medication, or to identify unusual or problematic situations [43]. Several health monitoring systems have been proposed to continuously measure health status information such as heart rate, electrocardiography (ECG), blood pressure, respiration, temperature, or oxygen saturation by wearable sensors [501, 494]. For instance, Pandian et al. [500] propose a remote health monitoring system based on a sensor vest that can measure ECG, blood pressure, temperature, photoplethysmography, and galvanic skin response. Chung et al. [159] combined a wearable chest sensor belt with a wrist pulse oximeter to measure ECG, accelerometer and oxygen saturation. Leijdekkers and Gay [402] utilize wearable ECG sensors to detect potential heart attacks. When a critical situation is detected, an application on the user’s phone asks for typical symptoms and, based on the answers, sends the user’s position and vital parameters to an emergency service. A mobile care system with autonomous alert function is proposed by Lee et al. [399]. Physiological information is stored and analyzed on a central healthcare server and can be accessed by physicians and healthcare providers. Different strategies allow for automatic emergency alerts in critical situations.

There are also several commercial products available that can measure different vital parameters and communicate them to remote caregivers or medical personnel. The Empatica wrist band [213] allows to measure heart rate, movements, temperature, and galvanic skin response and can communicate sensed data via a Bluetooth connected smartphone to a central server for statistical analysis. Continuous
monitoring of patients is provided by ZephyrLIFE HOME [706]. Alerts can be configured based on different sensor thresholds in order to notify clinical care teams. Sensed parameters include ECG, heart rate, blood glucose, respiration, body weight, activity minutes, posture, or burned calories and can be measured by different devices, e.g., a chest strap or a compression shirt with integrated sensors. SleepView [161] is a monitoring device for sleep apnea and home sleep testing, measuring body position, airflow, snore, and heart rate. Gathered information is uploaded to a web portal and analyzed by sleep technologists. Recent research aims to identify potential environmental causes of sleep disruptions by combining commercial sleep sensors with sensors for temperature, light, motion and audio [346].

Fall detection is another popular part of UbiComp applications in healthcare and assisted living. ICEdot [617] is a commercial bike crash sensor that detects serious falls. A sensor in the biker’s helmet detects changes in motion and forces, and sends the GPS position to preconfigured contacts in case of an emergency. While a detection of serious crashes is feasible, it is more difficult for normal falls of a person, e.g., during walking. However, for adults older than 65 years, unintentional falls are among the most frequent causes for fatal injuries and death [96]. Due to this fact, significant research is focusing on fall detection, trying to minimize the risk for elderly. Besides some already available products [116], most fall detection approaches are still a matter of research [704] and mostly focus on detection utilizing wearable accelerometers or gyroscopes [339, 486]. Accelerometer based approaches are also feasible with conventional smartphones as shown by Dai et al. [175]. This has the advantage that in case of an emergency an alert can be send to another person in order to call for first aid [618]. However, an evaluation of existing accelerometer-based fall detection approaches on real-world falls has shown that they are often inaccurate and lead to many false alarms [66]. Therefore, other approaches rely on video cameras and microphones [196], or depth cameras [628] to detect a sudden fall with higher reliability.

Other less emergency related applications aim at supporting medication [446, 183] or remote monitoring of daily activities by family members [551] or caregivers [517], sometimes even of activities in the bathroom [145]. To further enhance medication support, Proteus Digital Health is working on an ingestible sensor pill [84] that in combination with wearable sensors and Bluetooth LE technology [103] could capture the exact time of ingestion, heart rate, or activity [525].
former sections. In this respect healthcare applications are among the most popular existing UbiComp systems. Also the prevalence of smartphones has paved the way for many context-aware applications from different domains. This process will be further supported by the current rise of wearable devices with different sensors, like smart watches [678], fitness trackers [676], smart shoes [366, 276] or even smart socks [585], which are able to gather context information and can already recognize activities such as sitting, standing, walking, or biking. Some wristbands aim to support ubiquitous gesture control [379] and heart rate based authentication [97]. Another category of wearable devices pose smart glasses that are typically equipped with a head mounted display, WiFi or Bluetooth, and a camera in order to augment a user’s environment or to record moments of everyday life [677].

In our home environments we see the raise of more and more networked appliances, like smart TVs [243], smart lamps [518], or hi-fi systems [610]. Also the demand on home automation systems is increasing and deployments are expected to grow by 60% until 2017 [24]. While there are many vendors for professional but mostly expensive home automation and smart home solutions [165, 671, 57, 554], do-it-yourself projects [425] in the context of smart homes have become popular with the emergence of cheap, extensible, and simple to program hardware platforms like Arduino [53] or the Raspberry Pi [529], which are also popular platforms in the research community allowing rapid prototyping. Commercial do-it-yourself solutions are often based on the interplay of smartphones and appliances for simple retrofitting of existing infrastructure. Those solutions already allow to build smart scenarios, e.g., remote controllable door locks that automatically open when residents are in proximity [51], send notifications or even allow a live video connection when someone rings the door bell [195]. More sophisticated wireless video cameras for the home allow live monitoring of rooms, context-aware cloud recording based on a user’s location, and can send notifications based on learned activity patterns [197].

In recent years, a number of startups have emerged that aim at bringing an affordable internet of things to the home. The SmartThings Hub [600], Ninja Blocks [481], Twine [633], and Knut [47] are wireless networked mini-computer boxes that can be equipped with or connected to different sensors, e.g., to measure vibration, motion, humidity, or light. The boxes can be programmed by different rule-based languages (some work also with the web-based trigger and action service IFTTT [317]), for example to send an SMS when the washing machine finished, the temperature is too cold, or a water leak was detected. In combination with wireless networked power or light switches, e.g., the Belkin WeMo [83], or wireless connected thermostats [471], home appliances can also be controlled by these
boxes. They support several wireless radio technologies and different protocols to control existing smart home infrastructure, e.g., based on Z-Wave [596] or ZigBee [710]. Another related product is *mother* [584], a set of small connected sensors (so-called *cookies*) to gather several information items of daily life, e.g., medication, drinking and sleeping habits, or even teeth brushing performance. Collected data can be used to provide alerts, notifications, or just extensive statistics. The product is promoted by the auspicious but also daunting slogan “mother knows everything without needing to ask” [300].

The Ninja Blocks team aims at further enhance home automation by accurate in-home localization based on Bluetooth LE [103] and a gesture control interface. By using data from different sensors and actuators, the so-called *Ninja Sphere* [480] should be able to intelligently advice users and control home appliances.

Localization based on Bluetooth LE proximity sensing will be especially interesting for low-cost indoor location-aware applications. The *Estimote Beacon* [218] and *shopBeacon* [593] are early commercial products leveraging this technology in retail, e.g., to support customer localization, proximity marketing, check-in coupons, or contactless payment. They will enable retailers to notify customers about product details or special offers when they walk by. The low energy consumption of motes should allow them to run with a single battery for up to two years. The shopBeacon is currently deployed as a field trial in some retail stores in New York and San Francisco [421]. The beacon technology enhances already existing proximity sensing based on RFID, WiFi or cellular networks [442, 277]. Those technologies can be combined, e.g., as done by Radius Networks’ *Proximity Kit* [526], to notify application developers whenever users cross a predefined virtual boundary of a real-world geographical area (geo-fence).

Other domains where we see huge steps towards realizing the UbiComp vision are logistics and mobility. In logistics, for instance, the combination of RFID and GPS has been widely adopted to enhance tracking of products along the supply chain [536]. In the domain of mobility, we see ever smarter cars which are not only able to assist in parking, or line and distance holding, but are already able to drive autonomously by the use of GPS, radar, high-definition stereo cameras, and some other sensors [311]. More and more cars are connected to the Internet and are able to guide drivers to the nearest mechanic, fuel station, proactively navigate around traffic jams, or warn about critical situations. The focus is mostly on providing more safety and efficiency in mobility.

The fast technological progress is advancing many parts of Weiser’s UbiComp vision in our everyday life. UbiComp is not anymore only a matter of research but already present and relevant in many today’s applications of the real-world.
While UbiComp already found its way into our everyday life there are still several open challenges and general implications, which will be briefly discussed in the following section.

In general, UbiComp systems inherit the same technical challenges as distributed systems and mobile computing systems, e.g., remote communication, mobile networking, high availability, or energy awareness [565, 174]. Major technical challenges remain in terms of standardization and middleware support. Although existing technology already supports the development of complex and sophisticated UbiComp systems, most of them remain isolated application-specific solutions. The heterogeneity of communication technologies, protocols, software frameworks, and hardware platforms, hampers the interoperability of different UbiComp systems [174]. Standardization efforts are required in order to reuse and combine software and hardware parts of different UbiComp systems. As most middleware approaches for UbiComp are still a matter of research, vendors and other stakeholders of UbiComp applications should push the development of open source middleware to bring UbiComp to the next level.

More specific challenges of UbiComp remain in terms of scalability, reliability, and security [174, 125, 227]. When hundreds or even more devices per room want to talk to each other [682], efficient bandwidth and resource management is required [558]. Together with a huge number of potential involved users and services, required resources could be immense. This further raises the challenge of manageability. Who will setup and maintain those hundreds of devices per room? Users should not be required to perform system administrator tasks [205].

Reliability is a fundamental challenge in UbiComp, especially when systems act autonomously and decide to trigger specific actions or service invocations. How does a system learn what users really want in specific situations? When is it possible to infer user intents and when should it statically provided? [565] How can a system avoid wrong decisions, and how reliable are decisions especially when it comes to uncertainty, which will be present in most real-world situations. Wrong decisions could have fatal consequences and more drastically reduce the acceptability of a system compared to conventional computing applications, which are not integrated into the real-world. Imagine a medication support system that instructs a user to take an overdose of medicine because it did not detect the previous medication correctly. Or imagine an emergency system that wrongly detects a fall of an elderly person and requests an emergency service. Those false alarms could drastically decrease users’ and service personal’s trustworthiness in those systems. Reliability and trustworthiness are also important for smart home applications where users typically per-
form private but also work activities [205]. For many of our everyday activities it will not be acceptable if a system crashes or makes wrong decisions. While errors and system crashes of conventional desktop applications have been encountered by most users and are sometimes accepted as part of desktop computing, this differs to the expectation of reliability for other appliances in our real world. For instance, most users would not accept a system failure of a washing machine every second day, a malfunctioning coffee machine, or even a car. UbiComp systems are required to provide similar reliability as common household appliances.

Security mechanisms are required in order to ensure availability, integrity, and confidentiality of UbiComp systems [174]. Basic procedures for achieving these security properties rely on identification (of the user), authentication (verification of a claimed identity), and authorization (granting of access rights) [622]. However, those procedures become more complicated the more devices, users and services come into play. While in conventional desktop scenarios, confidentiality of data was typically assured by a single personal device, in UbiComp scenarios the same data could be distributed among many different devices and services and thus confidentiality needs to be guaranteed by each of them and for all involved communication channels. Same is true for protecting data integrity on multiple devices and services. As devices move more and more into the physical world, physical tamper protection becomes an important requirement [622].

How can we assure that a device was not replaced by a malicious one or modified with malicious components? Even harder to solve is the problem of protecting availability in UbiComp systems. While wireless communication technologies are vulnerable to jamming attacks, the ever increasing complexity of many communication protocols further allows more sophisticated and efficient deny-of-service attacks which are hard to detect [19]. Especially for critical UbiComp applications these vulnerabilities need to be addressed to assure availability.

Besides the technical challenges, UbiComp raises also several social and ethical implications [205, 104]. Those implications are often not foreseeable as they depend on how technology influences existing social conventions in real-world situations. Like earlier technological developments changed the way we perform domestic work (e.g., by the invention of the washing machine or microwave) or the way we communicate with each other (e.g., by the invention of the telephone, SMS, or E-Mail), UbiComp applications have the potential to change even more of our social life. An important aspect in this respect is the invisibility of UbiComp systems. While people are familiar with explicit interaction and control of conventional computing systems, UbiComp systems will provide implicit interaction and proactive adaptation based on gathered context information [574]. This form of sup-
port by a computing system will be completely new for most users and raises several questions, especially in terms of privacy.

Implications for the privacy of users have been discussed since the very beginning of UbiComp and were highlighted by many researchers [388, 80, 396, 381, 392]. Already in his often cited paper [682] Marc Weiser stated that his envisioned scenario “points up some of the social issues [...]. Perhaps key among them is privacy: hundreds of computers in every room, all capable of sensing people near them and linked by high-speed networks, have the potential to make totalitarianism up to now seem like sheerest anarchy.” We discuss the concept of privacy as well as its implications in the context of UbiComp in the following chapter.

2.6 SUMMARY

Marc Weiser’s vision of ubiquitous computing (UbiComp) has for many years influenced research efforts in many different domains. Technological developments over the past decades have paved the way for many existing real-world UbiComp applications, from smart environments to mobile and wearable assistance systems. While those systems provide reasonable support for different use cases and could make our lives more efficient, safe, healthy, and comfortable, they also pose new risks for our privacy.

The context-awareness of UbiComp systems relies on sensing and processing a multitude of information about users and their environments, which in many cases happens invisible due to the embedded and unobtrusive nature of those systems. The often involved context-based actuation and interaction capabilities can further cause disturbances which affect privacy by undesired interventions in a user’s environment. The following chapter will provide an overview of privacy definitions and dimensions before discussing privacy implications of UbiComp in detail.
Privacy has been discussed from social and legal perspectives for a long time. Early legal privacy considerations date back to the British Justices of the Peace Act from 1361 [453], or the English common law established in 1628, which is the source of the popular phrase my home is my castle [288]. Since then, the term privacy went through legal, social, economical, and technological changes over multiple centuries, which formed the understanding and expectations of privacy in different ways. Even if today everyone has an individual understanding of privacy and also several definitions from legal, social, and technical domains exist, there is yet no commonly agreed definition of the term. This chapter discusses the common dimensions of privacy reflected by different definitions and theoretical frameworks. After an overview of privacy principles and legal aspects, we discuss the inherent privacy implications of UbiComp in detail. The discussion is completed by the results of two studies in which we investigated users’ awareness about privacy implications stemming from already ubiquitous technologies today.

3.1 THE VALUE OF PRIVACY

The revelations of Edward Snowden in 2013 and 2014 about massive surveillance activities [383, 384] carried out by the U.S. National Security Agency (NSA) have attracted a lot of attention around the world. A common and ever-recurring argument for those and similar surveillance programs is that security outweighs privacy. In relation to the NSA activities, Barack Obama stated “you can’t have 100 percent security and also then have 100 percent privacy and zero inconvenience” [613]. However, as argued by security expert Bruce Schneier the debate should not be about security versus privacy, it should be about liberty versus control: “If the government can spy on their people; it reduces the people’s power, reduces liberty. If the government has to be open transparency, it reduces the government power, increases liberty” [68].

Another often heard argument is “if you aren’t doing anything wrong, what do you have to hide?” [575]. In 2009 Google CEO Eric Schmidt stated “if you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place. If you really need that kind of privacy, the reality is that search engines – including Google – do retain this information for some time and it’s important, for example, that we are all subject in the United States to the Patriot Act and it is possible that all that information could be made available to the authorities” [452].
Snowden’s information showed that this is already done on a larger scale than ever expected. However, the problem with these and similar arguments is their implication that privacy is about hiding something wrong [575, 608]. Privacy is not about hiding wrong doings. It is rather an inherent human right, which “protects us from abuses by those in power, even if we’re doing nothing wrong at the time of surveillance” [575].

Privacy is also important for philosophical, psychological, sociological, economical, and political reasons [607, 431]. The aim for individual autonomy, self-determination, private space, liberty of speech, and freedom of opinion are closely related to the need for privacy and democracy. Privacy supports social interaction and self-definition [45]. It allows self-assessment and exploration. It is the basis for development of individuality, and provides opportunities to relax or to recover from mental sorrow [686]. From a survey on different privacy perspectives in anthropology, psychology, and sociology, Boyle and Greenberg [109] found that privacy has been described as:

- “a basic human need,”
- “an institutionalized phenomenon,”
- “a state in which people find themselves,”
- “a quality of places, and”
- “a behavioral process governing interactions that seek to balance risks and rewards associated with social interactions.”

These descriptions highlight the complexity and diversity of perceived privacy values, which might be influenced by many factors.

One important factor is the technological progress [38]. While it allowed the affordable deployment of a world-wide surveillance infrastructure on the one hand, it also brings new opportunities as the ones related to novel UbiComp applications on the other hand. Those developments could change our expectations of privacy with new ways of interaction and communication. Langheinrich stated “shifts in technology require us to rethink our attitude towards privacy, as suddenly our abilities to see, hear, detect, record, find and manipulate others and their lives is greatly enhanced” [392].

Thus, while individual expectations and perceived value of privacy are manifold and influenced by many aspects (e.g., social, cultural, or technological factors), there is also no consistent understanding of the term privacy. In the following section, we discuss existing theoretical frameworks and privacy models in detail.
3.2 THEORETICAL FRAMEWORKS AND PRIVACY MODELS

Over the years, privacy has been analyzed from legal, philosophical, social, and technical perspectives [505]. From a philosophical point of view, privacy is an ethical concept [576] and, as stated by Warren and Brandeis [681], can be legally considered as an individual’s right in terms of the liberty to be left alone.

From a social point of view, privacy is based on the behavior and interactions between individuals, which are influenced by psychological and cultural properties [577]. From a technological perspective, privacy is often limited to aspects of information privacy. On the other hand, common social privacy frameworks are based on the concept of places, boundaries, and the dynamic regulation of boundaries based on individuals’ needs. We discuss the different privacy dimensions and related theoretical frameworks in the following sections.

3.2.1 Dimensions of privacy

While there have been many attempts [607] to define the term privacy, some researchers argue that “no definition of privacy is possible, because privacy issues are fundamentally matters of values, interests, and power” [685]. However, even though this statement was given by Alan Westin in 1995, today’s most common understanding of privacy as information privacy refers to his often cited definition from 1967 [686]:

“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

This privacy dimension, which also involves data privacy [78] or data protection [90], has become increasingly important with the widespread deployment of information technology and computers in many domains (e.g., government or healthcare). Information privacy gained further attention with the popularity of the Internet yielding many information-processing web applications and platforms, e.g., online shops and social networks. Also the growing prevalence of smartphones affects information privacy, as more and more information about users can be gathered and communicated in real-time around the world. An often investigated information is the location of users, which attracted considerable research on location privacy protection mechanisms [370].

The rapid development of information and communication technology makes it increasingly difficult for individuals “to determine when, how and to what extent information about them is communicated to others” [686]. This determination will become even more difficult in UbiComp when many invisible sensors and services gather, process and communicate information about users.
While information privacy is an essential issue in UbiComp applications, it is only one dimension of privacy [487, 185]. As Solove stated, “the theory of privacy as control over information excludes many aspects of life that we commonly assume to be private” [604].

From a more traditional point of view, privacy can be understood as “the more general right of the individual to be let alone” [681]. This popular privacy definition by the lawyers Warren and Brandeis from 1890 reflects the fact that privacy is not only about control of personal information but also about control of personal space and “the selective control of access to the self” [45]. As stated by Cohen [162], “privacy has a spatial dimension as well as an informational dimension.” The spatial dimension “encompasses both the arrangement of physical spaces and the design of networked communications technologies” [162]. This dimension involves aspects of solitude [416, 99, 111] and physical access [607] and is often referred to as territorial privacy [254, 209]. Rosenbaum [547] defined territorial privacy as:

“One’s right to be physically left alone or undisturbed. Territorial privacy is exemplified in the legal principles of trespass, real estate, and national sovereignty. This view of privacy allows one to impose physical boundaries around one’s proprietary space to avoid the interference of other people or their effects.”

Thus, territorial privacy “concerns the setting of limits on intrusion into the domestic and other environments” [209]. In everyday life people conventionally leverage spatial and physical features to set these limits, e.g., by opening and closing doors or blinds [577]. With respect to this, Boyle et al. [111] define a personal space as an “invisible boundary in space around a person, separating him from others.”

As Rosenbaum’s [547] definition suggests, territorial privacy also involves the physical aspect of being undisturbed in a personal space. Brey [114] defines such disturbances as “physical intrusions, in which privacy is violated through physical interventions.” Altman’s [45] definition of solitude is generalized by Boyle and Greenberg [109] as “control over where one directs one’s attention and how one controls distraction.”

In the context of the work place, Brill et al. [118] further classify similar privacy aspects into control over accessibility (e.g., for visitors or phone calls) and control of visual distractions and interruptions. Birkhoff et al. [99] describe this aspect as the “control over information moving toward the self (including interruptions), and determines how much of one’s attention is consumed by that information.” The Oxford English dictionary keeps the definition of privacy quite simple, but also involves those physical aspects by describing privacy as “a state in which one is not observed or disturbed by others.” [489]

Babbitt et al. [63] discussed physical privacy concerns in UbiComp environments and stated that “actuation of devices and objects in a user’s environment can intrude upon physical privacy [by] creating unwanted dis-
turbances.” Next to data sensitivity (information privacy), they identified three additional principles of physical privacy in UbiComp [63]:

- **Silence**: Separation from undesired noise and audio stimulus in the user’s environment in order to rest or relax.
- **Personal space**: Separation from the presence and activity of others. Withdrawing not only from noise but also from the proximity and actions of others.
- **Sovereignty**: Maintaining a sense of independence and autonomy. Controlling devices in the environment.

Similar physical privacy aspects that are closely related to a person’s body are also referred to as bodily privacy [254, 209] or privacy of the person [160] and concern “the protection of people’s physical selves against invasive procedures” [209]. With respect to UbiComp, Langheinrich stated [392]:

> “UbiComp has made those seemingly long-solved issues of bodily and territorial privacy become highly relevant again: Smart appliances, wearable computers, and activity recognition algorithms allow one to invade the bodily and territorial privacy of another person – not with one’s own eyes and ears, but from a distance that had previously constituted the realm of communication and information privacy.”

This statement highlights the fact, that UbiComp raises a multi-dimensional privacy problem and thus requires not only investigations from an information-centric point of view, but also from a user-centric point of view involving physical aspects of territorial privacy. Bok [105] defines this multi-dimensional view of privacy in terms of access control as “the condition of being protected from unwanted access by others – either physical access, personal information, or attention.” Smith [602] also tries to cover information and territorial privacy dimensions in his definition of privacy as “the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves.” Solove [606] formulated a privacy taxonomy which captures aspects of information privacy (collection, processing, dissemination) and aspects of territorial privacy (intrusion, interference) in order to support a better understanding of privacy in law.

### 3.2.2 Territories and boundaries

The territorial privacy dimension suggests that privacy is closely related to physical constraints, such as territories and boundaries. From a social perspective, Edney and Buda [204] describe territoriality “as a
set of behaviors which a person (or persons) displays in relation to a physical environment that he terms as “his” and that he (or he with others) uses more-or-less exclusively over a period of time.” Such territories can be physically demarcated, e.g., by walls and doors of a room or a house, or virtually demarcated by social and cultural conventions [204]. A virtual demarcated territory is also referred to as a space [281, 588], or a portable territory [279].

Hall [281] defines four types of different spaces around a person in relation to the distance: intimate space, personal space, social space, and public space. The entry into the intimate space is only acceptable for closest friends. While the personal space is used for conversations with friends and family members, the social space is for any other interactions with acquaintances and strangers. The public space relates to the space in which an individual perceives interactions as impersonal and anonymous.

A violation of privacy occurs, when a person who is not desired to participate in a space enters it, or when a person undesirably crosses the borders of a defined space or territory. Marx [439] describes border crossing as a core concept of perceived privacy violations. In addition to physical or natural borders, he discusses three further borders which could be crossed to cause privacy violations:

- **Natural borders** refer to physical borders which typically protect what someone can perceive by “natural” senses (e.g., what someone can see and hear). Such borders are clothes, walls, darkness, spatial distance, or a sealed letter.

- **Social borders** are based on the social expectations and trust in social roles, (e.g., a close friend, family member, or doctor) and are crossed when confidentiality of information is breached.

- **Spatial or temporal borders** refer to the disconnection of separated locations and point in times with all its involved information. Those borders are crossed when information is connected among space and time.

- **Transitory borders** assume that interactions or communications are transitory and do not persist when they have been terminated. Hidden recordings (e.g., by surveillance systems) would cross such borders.

Technology eases the way of how those different borders can be crossed and could even contribute to a decreased effectiveness of borders. Especially natural borders can lose their meaning of privacy protection. Mancini et al. [429] discuss how the fact that “borders of physical and virtual places are becoming progressively blurred,” leads to new socio-cultural boundaries, e.g., when using online social networks. They identify personal policy, inside knowledge, etiquette, proxemic, and
aggregation boundaries, which are frequently used by members of online social networks to set privacy demarcations. Those boundaries are primarily defined by socio-cultural knowledge, functions, relations and rules [429]. Based on Altman’s boundary regulation theory [45], Karr-Wisniewski et al. [695] define five related boundary types for online social networks: relationship, network, territorial, disclosure, and interactional. The physical dimension of privacy with its involved disturbances is addressed by the territorial boundary which regulates incoming content, and by the interactional boundary which regulates potential interaction and overall access of oneself to specific individuals [695].

The problem of dissolving physical borders in cyberspace depicts also a problem in law as “traditionally, privacy has been inextricably linked to physical space” [28]. Abril argues that “instead of physical space, we should think in terms of walls of confidentiality built by technical architecture, agreements, and relational bonds” [28].

Shapiro [588] explores how new information and communication technologies affect the natural boundaries of the home. He states that “it may be more profitable to think of privacy […] in terms of the confluence of various boundaries, both physical and virtual.”

The pervasive sensing and communication capabilities of UbiComp systems will contribute even more to dissolving natural borders. Kindberg and Fox [356] claim that designers of UbiComp systems “should divide the UbiComp world into environments with boundaries that demarcate their content. A clear system boundary criterion – often, but not necessarily, related to a boundary in the physical world – should exist.” A similar idea for UbiComp is expressed by Langheinrich [388] who states “that one would require that information is not disseminated indefinitely, even not across a larger geographic boundary, such as buildings or rooms. Information collected in a building would stay within the building’s network.” The idea of demarcating information boundaries and limiting the flow of information is also reflected in the terms “physical or virtual informational space” [701], “information space” [330], “digital territories” [177], or “virtual walls” [342].

Palen and Dourish [498] define three boundaries (disclosure, identity, and temporal) for privacy management in a “networked world”. From an information-centric perspective the disclosure boundary determines what information is disclosed under what conditions. The identity boundary is required to support the disclosure boundary by managing the own identity disclosed to users and by managing receivers of disclosed information. Similar to Marx [439], the temporal boundary is associated with past, present, and future treatments of disclosed information.
3.2.3 Dynamic regulation

Privacy regulation and decision making is not a static but highly dynamic and context-dependent process, as recognized by Westin [686] and Altman [45]. Westin states that “each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication” [686]. Also sociologist Altman [45] describes privacy decision making as part of his privacy regulation theory as a “dialectic and dynamic boundary regulation process,” that is traditionally performed by utilizing “features of the spatial world and the built environment, whether that be the inaudibility of conversation at a distance or our inability to see through closed doors [and] behavioral norms around physical touch, eye contact, maintenance of interpersonal space, and so on” [45]. Altman describes inputs and outputs as properties of an individual’s engagement in social interactions. When the amount of inputs and outputs is on an accepted level, the achieved privacy equals an individual’s desired privacy. Whenever this balance is violated a privacy state is either crowded (too many interactions) or isolated (too few interactions), according to Altman [45].

Both, Westin’s and Altman’s theoretical work have influenced much research [432]. Stanton and Stam [624] combine Altman’s boundary regulation theory with social exchange theory to predict an individual’s motivation to reveal or withhold information. They suggest the concepts of boundary opening and boundary closure as “dynamic, psychological processes of regulation by which people attempt to control flows of valued information to other people in their social environments” [624]. Karr-Wisniewski et al. [695] investigated Altman’s theory in the context of OSNs and found that users achieve boundary regulation by different strategies, such as filtering, ignoring, blocking, or compliance. Similar preventive and corrective boundary regulation strategies for OSNs have been identified by Lampinen et al. [382]. They found that in addition to individual control strategies, collaborative strategies are particularly becoming important, e.g., negotiation of sharing and access to photos.

Palen and Dourish [498] apply Altman’s theory to today’s world of networked information technology. They highlight the complexity of boundary regulation in that context by stating that:

“Privacy management is not about setting rules and enforcing them; rather, it is the continual management of boundaries between different spheres of action and degrees of disclosure within those spheres. Boundaries move dynamically as the context changes. These boundaries reflect tensions between conflicting goals; boundaries occur at points of balance and resolution.”

Palen and Dourish recognize that “information technology can create intersections of multiple physical and virtual spaces,” and thus Altman’s
traditional boundary regulation strategies leveraging spacial properties are no longer effective. However, they focus on information-centric boundaries and do not discuss the physical privacy dimensions which are of particular interest in UbiComp.

In the context of UbiComp systems, Boyle [108, 111] deconstructs Altman’s theory into three control modalities used for privacy regulation: solitude (controls interpersonal interactions and attention), autonomy (controls observable manifestations of identity), and confidentiality (controls information access and fidelity).

Also Lehikoinen et al. [400] extend Altman’s theory to address dynamic privacy regulation in UbiComp by mapping his concept of inputs and outputs to different UbiComp interaction types. They further apply Altman’s boundary control mechanisms of territory and personal space to UbiComp. In their understanding, territory in UbiComp refers to the ownership and control of a geographical area, objects, embedded devices, and available services in the environment. Personal space is extended by personal devices as mediators for more types of interactions in UbiComp, and a digital self referring to personal information of an individual [400]. They discuss how these concepts relate to different control mechanisms (e.g., access control, management of visibility, and filtering) for privacy regulation in typical UbiComp scenarios. Adams and Sasse [35] propose the privacy invasion cycle as a model for user perceptions of privacy in multimedia environments. They state that “most invasions of privacy occur when users realize that a mismatch has occurred between their perceptions and reality.” The invasion cycle is influenced by users’ previous experiences, their role in an interaction, and their perception of information sensitivity, information receivers, information usage, and context of interaction. Because these factors are all subject to change, this model does also reflect the dynamic nature of privacy regulation.

3.2.4 Territorial privacy

The previous discussion of different privacy definitions and theoretical privacy frameworks highlighted the multi-dimensionality of privacy, which involves an information-centric dimension as well as user-centric physical dimension. While the information-centric dimension covers privacy invasions with respect to the undesired access of personal information, the physical dimension covers privacy invasions with respect to undesired access to the self. Most theoretical work on privacy addresses only one of both privacy dimensions. However, the integration of UbiComp technologies in our everyday environments raises both informational and physical privacy issues and therefore requires addressing privacy from a holistic point of view.

In this work, we address both of these privacy dimensions by respecting privacy invasions in UbiComp in terms of observations and
Based on the discussed theoretical backgrounds of privacy, we define observations as the act of accessing personal information of a user. This involves the collection, communication, or processing of personal information. However, with respect to UbiComp systems, the collection focuses on information that is gathered by different user-centric or environment-centric sensing technologies as discussed in Section 2.2.4. Furthermore, we define disturbances as the act of accessing a physical space or the attention of a user. Such an access can be caused by automation, actuation, or interaction capabilities of UbiComp systems as discussed in Section 2.2.5. With respect to the previously discussed concept of border crossings, one can consider observations as outgoing border crossings and disturbances as incoming border crossings.

Another limitation of most former privacy definitions is their focus on privacy as the act or the right of control. We argue, however, that the awareness of privacy implications should also be a fundamental part of the right to privacy. While control to some extent implies the need of awareness, we believe that awareness should be an explicit part of a privacy formulation.

Consequently, we combine the notion of observations, disturbances, awareness, and control to define our understanding of territorial privacy in UbiComp, which will be used throughout this thesis:

**Definition 1** Territorial privacy is an individual’s right to be aware of potential observations and disturbances as well as an individual’s right to control undesired observations and disturbances.

### 3.3 Privacy Legislation and Privacy Principles

Privacy laws and principles have been adapted around the world since the advent of information technology. Therefore, most of those laws and principles focus on the protection of information privacy and are motivated by the early work of Warren and Brandeis [681], as well as the work of Westin [686] (see previous Sections 3.2.1 and 3.2). Especially in the context of privacy legislation, many scholars agree that Warren and Brandeis’ article is the foundation of privacy law in the United States [605].

The first data protection law in the world was passed by the German federal state of Hesse in 1970 [386]. However, more influential for later privacy legislation were the fair information practices (FIPs) of the US Department of Health, Education and Welfare from 1973 [36], which resulted in the US privacy act of 1974. The advisory committee proposed five FIPs, which they considered to be “the minimum set of rights that should be available to the individual” [36]:

-
### 3.3 Privacy Legislation and Privacy Principles

Today a large number of countries have information privacy laws which are based on the FIPs [268] and also several other guidelines and principles for privacy protection were influenced by them (see Figure 3.1). With respect to UbiComp, those principles and guidelines define statements that should be either applied at the user level or system level of UbiComp systems. At the user level these statements support privacy *awareness* and *control*, while at the system level they support *enforcement* of privacy decisions.

#### Figure 3.1: Popular privacy guidelines and principles in UbiComp. The figure shows the relation between different principles from legal and technical domains. It further highlights their classification into privacy awareness and control principles at the user level, and into privacy enforcement principles at the system level.

1. “There must be no personal-data record-keeping systems whose very existence is secret.”

2. “There must be a way for an individual to find out what information about him is in a record and how it is used.”

3. “There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.”

4. “There must be a way for an individual to correct or amend a record of identifiable information about him.”

5. “Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.”
The Organisation for Economic Cooperation and Development (OECD) relied on those FIPs as core principles for creating their Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980 [488]. The guidelines state eight principles together with numerous other and similar sets of privacy protecting rules [488]:

1. **Openness Principle** “There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.”

2. **Purpose Specification Principle**: “The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”

3. **Individual Participation Principle**: “An individual should have the right:
   a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
   c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
   d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.”

4. **Collection Limitation Principle**: “There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.”

5. **Use Limitation Principle**: “Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification principle except with the consent of the data subject, or by the authority of law.”
6. **Data Quality Principle**: “Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.”

7. **Security Safeguards Principle**: “Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.”

8. **Accountability Principle**: “A data controller should be accountable for complying with measures which give effect to the principles stated above.”

The OECD guidelines in turn have been adopted as part of many international privacy regulations, including the European Union’s (EU) Data Protection Directive 95/46/EC [223] from 1995 and the Canadian PIPEDA\(^1\) law [261]. The EU Directive frames a common understanding of privacy principles to be used in legislation of the EU’s member states. While the Directive is grounded in the FIPs and OECD guidelines, it refines those principles further and adds the criteria of explicit consent in article 7 [223]: “Member States shall provide that personal data may be processed only if the data subject has unambiguously given his consent […]”. To cope with new technology driven privacy problems the EU also proposed the e-Privacy Directive 2002/58/EC [224] based on the Telecommunications Privacy Directive of 1997. The directive was amended in 2009 and regulates “traffic data” (e.g., the processing and storing of IP addresses) and “location data” (e.g., the geographical position estimated by communication technologies). Currently, the European Union is working on a reformation of their data protection rules to foster important privacy practices such as the right to be forgotten, easier access to own data, or privacy by design [219, 220].

The US Federal Trade Commission’s (FTC) Fair Information Practice Principles (FIPs) [385] from 1998 reframe the first version of FIPs in order to represent the common concerns about information privacy in the World Wide Web. The Commission defined five core principles of privacy protection [385]:

1. **Notice/Awareness**: “Consumers should be given notice of an entity’s information practices before any personal information is collected from them. Notice should include: identification of the entity collecting the data; identification of the uses to which the data will be put; identification of any potential recipients of the data; the nature of the data collected and the means by which it is collected if not obvious; whether the provision of the
requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.”

2. **Choice/Consent:** “Choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information – i.e., uses beyond those necessary to complete the contemplated transaction.”

3. **Access/Participation:** “Access […] refers to an individual’s ability both to access data about him or herself – i.e., to view the data in an entity’s files – and to contest that data’s accuracy and completeness. Both are essential to ensuring that data are accurate and complete.”

4. **Integrity/Security:** “Data [should] be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form. Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.”

5. **Enforcement/Redress:** “The core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. […] Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.”

While those and similar principles have been adopted by many states in national laws during the past decades, the rapid technological changes often provide new challenges not respected in existing law. A recent investigation of civil society groups, industry and international experts tried to address these challenges by proposing international privacy principles on the application of human rights to communications surveillance [208]. In addition to similar principles as described before (e.g., transparency, user notification, and integrity), they propose further principles to cope with inappropriate governmental surveillance practices (e.g., legality, necessity, proportionality, or public oversight). In the US, the recent developments in flying drones equipped with high resolution cameras [253] has lead to similar specialized privacy principles as defined in the first Drone Aircraft Privacy and Transparency Act of 2013 [433] to limit data collection.
The effectiveness of existing privacy legislation will be challenged even more by novel UbiComp technology. With the beginning of UbiComp research, Bellotti and Sellen [86] recognized the need for user-centered privacy guidelines when designing UbiComp systems. They identified feedback and control as the two major privacy principles of the user level (see Fig. 3.1). While feedback is required to inform “people when and what information about them is being captured and to whom the information is being made available,” control should “empower people to stipulate what information they project and who can get hold of it” [86]. Bellotti and Sellen distinguish between four factors that should be respected by feedback and control mechanisms in UbiComp:

1. **Capture:** When and what kind of information is captured?

2. **Construction:** What happens to information (e.g., processing, aggregation, encryption, storage)?

3. **Accessibility:** Who and what has access to what information?

4. **Purpose:** What is the intention of those who wish to use information? How might it be used in the future?

Adams [34] proposes similar feedback and control design recommendations for privacy in multimedia environments. They highlight the need to inform users about the captured data (e.g., images, video, audio, or degree of distortion), data usage (recording, transmission, (re)usage, and purpose), and the data receiver (identity, physical and organizational distance to a receiver) as the most important factors.

Appropriate feedback and control mechanisms are also requested by Jiang et al.’s [331] Principle of Minimum Asymmetry stating that “a privacy-aware system should minimize the asymmetry of information between data owners and data collectors and data users, by:”

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

The invisible nature of UbiComp typically causes an asymmetry of information (collected information and feedback information) when data owners are not fully aware of data collection and data forwarding to other entities. Jiang et al. [331] discuss different approaches of prevention, avoidance, and detection, in order to minimize this asymmetry and avoid a mismatch between perceived and real privacy implications in UbiComp systems.

Based on the described FIPs and some enhancements of the EU Directive from 1995, Langheinrich [388] developed six privacy principles to support UbiComp system designers: notice, choice and consent,
access and recourse, proximity and locality, anonymity and pseudonymity, and adequate security.

While most principles have been discussed before, Langheinrich introduced two new principles: the proximity and locality principle and the anonymity and pseudonymity principle. The proximity and locality principle should cope with the problem that notices and explicit consent might be not feasible in several UbiComp scenarios. In such scenarios, privacy decisions could be coupled to the user’s proximity (e.g., only capture data in the user’s presence). Locality refers to natural borders (see Section 3.2.2) that can be used to limit the flow of information (e.g., tying information to the room or building it was captured). Anonymity and pseudonymity are well known principles in computer science and several approaches for achieving anonymity in the online world already exist [203]. However, in a real world equipped with UbiComp systems, such mechanisms are much harder to deploy (e.g., in video monitoring systems where it is hard to hide one’s real face). Therefore, Langheinrich considers anonymity and pseudonymity as an important principle for privacy in UbiComp on its own. He further points out that designers of UbiComp systems “cannot rely on lawmakers and sociologists to be fully aware of the vast possibilities and implications that the technology so obviously presents [. . . and that they] need to understand the potential and danger of [their] advancements, and develop sound conventions and guide-lines according to well-established principles that will help [them] drive technology into a responsible and socially acceptable direction” [388].

Based on Bellotti and Sellen’s [86] practical guidelines described above and on Palen and Dourish’s [498] theoretical work on dynamic privacy regulation (see Section 3.2.3), Lederer et al. [397] identified five common pitfalls for UbiComp system designers with respect to privacy implications. They argue that often the “designs of these systems inhibit peoples’ abilities to both understand the privacy implications of their use and to conduct socially meaningful action through them.” Regarding a user’s understanding of a system’s privacy implications, designers should avoid:

1. **obscuring potential information flow:** “Designs should not obscure the nature and extent of a system’s potential for disclosure. Users can make informed use of a system only when they understand the scope of its privacy implications.”

2. **obscuring actual information flow:** “Designs should not conceal the actual disclosure of information through a system. Users should understand what information is being disclosed to whom.”

To avoid these design flaws, Lederer et al. [397] advise designers to work on the alignment of users’ mental models of potential and actual information flow with the system’s and observer’s information
model. Their advice is motivated by Don Norman’s [485] popular work on the relevance of mental models in the design process of user interfaces. While the former two pitfalls relate to privacy awareness at the user level (see Fig. 3.1), the three other pitfalls describe how to provide better privacy control (“social meaningful action”) at the user level by avoiding:

3. **emphasizing configuration over action**: “Designs should not require excessive configuration to manage privacy. They should enable users to practice privacy as a natural consequence of their normal engagement with the system.”

4. **lacking coarse-grained control**: “Designs should not forgo an obvious, top-level mechanism for halting and resuming disclosure.”

5. **inhibiting existing practice**: “Designs should not inhibit users from transferring established social practice to emerging technologies.”

Like these and the former guidelines suggest, encouraging system developers to incorporate privacy considerations from the very beginning of a system design process is central to successfully build privacy-aware UbiComp systems. A prominent advocate proclaiming this privacy by design concept is Ann Cavoukian, the former Privacy Commissioner of Ontario in Canada. She defined seven foundational privacy by design principles and discusses how these can be followed in the design process of UbiComp applications [138]:

1. **Proactive not Reactive; Preventative not Remedial**
2. **Privacy as the Default Setting**
3. **Privacy Embedded into Design**
4. **Full Functionality – Positive-Sum, not Zero-Sum**
5. **End-to-End Security – Full Lifecycle Protection**
6. **Visibility and Transparency – Keep it Open**
7. **Respect for User Privacy – Keep it User-Centric**

All former principles and guidelines introduced so far were motivated by the dimension of information privacy and therefore lack specific statements regarding the physical aspects of territorial privacy (see Section 3.2.1). However, most principles can be considered under the dimension of territorial privacy as well. Babbitt et al. [63] have also identified this issue and proposed four principles “to drive the understanding of physical privacy” in UbiComp:
1. **Silence:** “Individuals may want to separate themselves from unwanted noise in order to rest or relax. Peace and quiet is a commonly desired condition that can be violated by sound-producing devices like speakers, radios, televisions, and phones. These types of devices may need to be temporarily disabled or muted to prevent unwanted audio stimulus in the user’s environment.”

2. **Personal Space:** “Individuals may desire separation from the presence and activity of others, wishing to withdraw not only from noise but also the proximity and actions of others. A desired amount of space can be violated if others enter a user’s environment. Preserving this goal by closing barrier objects such as doors, shades, or blinds can provide the conditions for this sort of spatial solitude.”

3. **Sovereignty:** “It is common to think of the devices and objects that an individual owns as his or her property, and it is a rarely questioned right of an individual to use their property as they see fit and have the ability and authority to determine how others use his or her things as well. This principle is especially important to maintaining a sense of independence and autonomy in such a networked and interoperable world that allows others in remote locations to actuate local devices.”

4. **Data Sensitivity:** “Actuated devices and objects can influence the levels of detail of personal information that can be collected by a user’s environment. Often, increasing the level of detail of personal information makes the data more privacy sensitive. For example, video images at night will likely not reveal much detail, unless a light is turned on, or turning off background noise (i.e. a television or radio) makes audio information more decipherable. Enforcing this principle requires knowing the impact of physical devices and objects upon the environment’s information gathering capabilities.”

The privacy principles of Babbitt et al. [63] describe territorial privacy aspects that should be respected at the system level of a UbiComp system (see Figure 3.1).

While all discussed guidelines and principles provide a good starting point for privacy requirements in UbiComp, in most cases they do only describe generic best practices. The many different facets of UbiComp scenarios and their involved privacy implications make it difficult to derive concrete mechanisms for providing privacy awareness and control at the user level as well as privacy enforcement at the system level from these principles. In the following section we will discuss the major privacy implications that we identified in typical UbiComp applications.
3.4 Privacy Implications of Ubicomp

As one of the major challenges of Ubicomp, privacy implications for users have been discussed since the very beginning of Ubicomp research [675, 388, 80, 396]. Already Marc Weiser [682] pointed out that privacy implications in Ubicomp directly stem from its main characteristic features, namely *invisibility, context-awareness, proactivity, and inter-connectivity*, see Figure 3.2.

In Weiser’s Ubicomp vision technology should completely disappear from a user’s attention. To allow this invisible computing in form of individualized user support, systems must sense context information about users in order to function as reliably as possible. This information can be “more intimate than ever before: not only what we do, where we do it, and when we do it, but also how we feel while doing so” can be of interest for Ubicomp systems [381]. The combination of different user-centric and environment-centric sensing technologies (see Section 2.2.4) with novel learning or data mining strategies further allow to infer new higher level information, which could not be gathered by any sensor directly. For instance, such approaches could enable the inference of private behaviors or lifestyle patterns from wearable sensors [141, 44], or even from humidity sensors [282] and smart meters [271, 549, 458] installed in home environments.

Furthermore, Ubicomp systems are expected to support everyday situations in real world environments with automation, actuation and interaction capabilities (see Section 2.2.5). This might involve the control of actuators in the user’s physical environment, either to adapt the environment or to attract the user’s attention for interactions by controlling visual, acoustic, or haptic output devices. In addition to environmental devices, e.g., home automation components or displays and speakers, in Ubicomp such devices might also involve normal everyday objects, e.g., wearable objects such as shoes [366] or necklaces [559]. In the home environment users can be further supported by autonomous robots, e.g., by cleaning robots [237] or
caregiving robots [589]. Furthermore, interaction in UbiComp is often facilitated through ambient output modalities, e.g., by public displays [466], personal projected displays [552], or by speech dialog systems [283], which enable pervasive interaction, everywhere and anytime.

However, the proactivity and autonomy of many UbiComp systems (see Section 2.3) can lead to undesirable adaptations and interactions especially when wrong decisions were made. Those undesired adaptations of devices or systems in the user’s environment can cause privacy-affecting distractions and disturbances. For instance, when a cleaning robot starts its cleaning process, blinds automatically close according to light conditions, a front door automatically opens for family members, voice interactions are started, or an acoustic notification is delivered while the user aims for relaxation at home.

Therefore, with respect to our definition of territorial privacy (see Section 3.2.4), a user’s privacy can be affected by many different observations and disturbances.

The invisible nature of embedded sensors and actuators further causes a mismatch between perceived privacy and real privacy implications stemming from UbiComp systems. How do users know that a system is present? How do users know what sensors are gathering information about them and what can be inferred from those sensors? How do users know what a system is going to do in a specific situation? It will become more and more difficult if not impossible for users to be aware of active sensors, existing actuators, and systems in their environment. Current developments in wearable sensing devices such as Google Glass [258] and the Narrative Clip [468] are only few examples of how sensing technologies are already invading our environments and pose novel privacy risks through invisible and unobtrusive image and video recordings [542].

Another privacy implication of UbiComp systems stems from their interconnection with other systems and services. The ubiquitous interconnectivity leads to the fact that physical boundaries dissolve as they lose their traditional function of demarcating and protecting a user’s privacy. Communication technologies allow to forward gathered information in real-time around the world and allow to control systems from any other location. Thus, instead of the demarcation by physical boundaries, privacy in UbiComp is demarcated by virtual boundaries of which users might not be aware of. In fact, UbiComp by its definition has the “potential to create an invisible and comprehensive surveillance network” [104].

Some researchers [544, 612] already argue that complete invisibility should not be the ultimate goal in UbiComp and more user engagement is required to “shift from proactive computing to proactive people” [544]. Especially the lack of awareness of active sensing technologies is often criticized in literature and is one of the major issues of
privacy implications in UbiComp [86, 27, 388]. This lack of awareness may lead to discomfort and the feeling of violated privacy expectations when users discover at a later state that they have been observed by a system, or that a system operated in an unexpected manner. Only if users are aware of potential privacy implications in terms of observations and disturbances they can decide whether to use a system or not, or decide what steps to undertake in order to control systems according to their privacy preferences [482].

In the following section we discuss the issue of missing or incomplete privacy awareness of privacy implications stemming from already existing technologies.

3.4.1 Awareness of technological privacy implications

While privacy implications in the real world can typically be perceived by natural borders (see Section 3.2.2), information technology and in particular UbiComp technology cause new and invisible privacy implications. Deployed systems often provide complex functionality with several different privacy implications that cannot be naturally perceived by users. This could lead to misunderstandings or even to complete unawareness of existing privacy implications.

The mismatch between mental models and system models has been shown in different user studies. Jensen et al. [329] investigated the online behavior of users in an experimental e-commerce scenario. They found that users’ perceptions of their own knowledge about privacy-relevant technology and involved privacy risks is often inaccurate. The EU’s large scale study on Attitudes on Data Protection and Electronic Identity in the European Union revealed that while 58% of Internet users usually read privacy statements on websites, many of them do not fully understand those statements. Similar results have been discussed by Ur et al. [661]. They conducted 48 semi-structured interviews about online behavioral advertising (OBA) and found that many participants were surprised of how browsing history was actually used by advertisers. Interestingly many participants believed that companies collected more information than they collect in general. The same was observed by McDonald and Peha [445] for OBA who further found that users often did not understand the functionality of their browser’s do-not-track (DNT) settings. In the context of the online social networks (OSNs), Acquisti and Gross [31] found that Facebook members had often a misunderstanding of the visibility of their own profiles and Facebook’s treatment of personal information.

Some research [520, 357] investigated users’ mental models of RFID technology and found that the functionality of RFID were not well

---

2 The do-not-track (DNT) function of browsers is realized by a specific HTTP header to signal websites that users do not want to be tracked, e.g., by cookies.
understood. This could lead to wrong assumptions about involved risks, less acceptance and less perceived benefit of this technology.

In an exploratory study Klasnja et al. [359] found that even though the technical details of WiFi technology were well understood by users, they did not understand important privacy risks, e.g., the visibility of data transmitted over an unencrypted WiFi network. The lack of awareness leads to insufficient protection practices and a false sense of security.

The potential severity of using unencrypted WiFi networks, has been demonstrated by our identified security flaw in Google’s ClientLogin protocol, which affected almost all (99.7%) Android users in May 2011 [378]. Authentication tokens for Google’s Calendar, Contacts, and Picasa services were transmitted unencrypted and allowed eavesdroppers to gain full access to these services. Thus, an adversary could view, modify or delete any contacts, calendar events, or even private pictures. The issue was fixed after the security problem had attracted global media attention.

Also the privacy implications of granted permissions to mobile applications are often misunderstood by users. For instance, users are often not aware that data is shared for advertising purposes [70], that applications can also invisibly run in the background [646]. Furthermore, most users are not able to infer the purpose of granted permissions at install time [409].

As already the privacy implications of today’s technology are hard to infer, it will become even harder for invisible UbiComp technology. The wrong assumptions and misconceptions about a UbiComp system can lower user acceptance, e.g., when users falsely assume that a system permanently records video [669]. The perceived purpose of a UbiComp system influences perceived privacy implications, but those purposes are often perceived incorrectly [417, 587]. Also the results from a larger deployment study of a UbiComp system in a US eldercare facility showed that both elderly and caregivers had misconceptions of the technology and thus wrong assumptions about privacy implications [80]: “users’ inability to see a technology makes it difficult for them to understand how it might affect their privacy.”

In the following sections, we discuss the results of two studies in which we investigated peoples’ awareness of privacy implications stemming from zero configuration networking and from presence sharing features in mobile messaging applications, respectively.

3.4.2 Study: Privacy implications of Zeroconf

Zero configuration networking (Zeroconf) aims to support users in seamlessly connecting devices and services in a local network, e.g., to connect a smartphone with a TV or a nearby printer at home. The conceptual requirements were specified by the IETF ZeroConf Work-
privacy implications of ubicomp

In order to realize host name resolution without a DNS server, and local service discovery without any rendezvous server. With Bonjour [52], Apple introduced one of the most adopted Zeroconf implementations, which proposes Multicast DNS (mDNS) [148] and DNS-based Service Discovery (DNS-SD) [147] as solutions for these requirements.

Host names are used in mDNS records to help users and hosts identify other hosts in the local network. Those names are periodically announced in the current network. A host name is typically composed of the device name, which in turn can range from pseudonyms that do not directly reveal any personal information about the user to device names that disclose the type of device, personal interests, as well as nicknames and full names of users (e.g., John-Doe’s-iPhone). Thus, the periodic announcement of host names can have varying implications on user privacy when a device is connected to a public or semi-public networks, depending on how the host name is composed.

Focusing on mDNS, we assessed this issue by studying its actual extent, awareness about the problem, and potential privacy risks [10].

Methodology

In order to investigate the potential impact of device names on user privacy, we collected a one-week dataset of mDNS announcements in a semi-public WiFi network at the university of Ulm campus in June 2012. According to prior agreement with our data protection officer, only necessary data was extracted from mDNS messages and partially anonymized before storage, i.e., only the hashed MAC address and the device name were stored. The collected dataset includes 2,957 unique devices and their device names.

We further conducted an online survey in order to better understand how users select their device names and if they are aware of privacy risks stemming from service announcements including device names. A total of 137 individuals aged 19-55 (Mdn=25) participated in our survey (32 female, 105 male). The majority of participants (65%) work or study in the ICT sector. Notebooks were owned by 130 participants; smartphones by 105. Three owned neither a notebook nor smartphone.

Results: scope and awareness

Of 2,957 unique device names, 59% contained real names of users, with 17.6% containing first and last name, see Table 3.1. In other words, almost two out of three device names contain at least a part of

The study has been jointly conducted as part of the bachelor thesis of Christoph Bachmaier [64].
the user’s name, if not even the complete name. A model name was found in 58% of all messages.

The online survey revealed that all participants had heard of Wi-Fi and had used it at some point, whereas 40% stated that they had never heard of Bonjour and 31% stated that they had heard about Bonjour but had never used it. However, most of the 54 participants (83%) who never heard of Bonjour did not own an Apple device, which suggests that most Apple users are aware of Bonjour. Out of the 43 participants who stated to have heard about Bonjour but have never used it, 14 (33%) did own an Apple device. As Bonjour is activated by default on Apple devices, it is fair to assume that these persons as well as the Apple users who never heard of Bonjour had used it at some point in time without being aware of it.

Using Spearman’s rank correlation, we analyzed survey replies in relation to expertise (Wi-Fi, Bluetooth, UPnP and Bonjour) and privacy proclivity (based on Westin’s privacy indexes [373]) of participants. Concerning the awareness about device names being periodically announced in local networks for service discovery, we found no correlation between awareness and privacy proclivity. However, awareness of this problem is significantly higher with increasing level of expertise ($r=0.43$, $p<0.01$, $n=61$). This aligns with expectations that participants with deeper technological understandings know about the announcement of device names, while privacy fundamentalists may have a strong desire to protect privacy but may lack the knowledge for doing so.

We further found that 29% of the participants did not know the current device name of their smartphone, but that the vast majority considered periodic announcement of their full names worrisome. Overall, 32% of the participants were not aware that this name was transmitted in local networks as part of Zeroconf protocols. While those numbers seem relatively low, it must be respected that the majority of participants (65%) had a computer science background. A detailed discussion of the results can be found in [10].

Privacy threats & attack scenarios

In the following, we highlight the potential privacy risks by discussing a number of specific threats and attack scenarios enabled by Zeroconf announcements.

In smaller public Wi-Fis with a limited number of users, the announcement of a device name could directly identify a person. For instance, Alice is sitting with her iPad in a cafe with free Wi-Fi and is the only person using an iPad. Her device name is configured as Alice-Doe’s-iPad. If Bob wants to know her name, he just needs to connect to the same Wi-Fi network, start a Zeroconf browser and search for Alice’s iPad. Now Bob could gather background information about her social profile with online searches, and approach her as an old
Table 3.1: Categorization and distribution of mDNS device names from our dataset containing 2,957 unique devices.

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
<th>total #</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 full name with model name</td>
<td>John Doe’s MacBook Pro</td>
<td>420</td>
<td>14.2</td>
</tr>
<tr>
<td>2 full name</td>
<td>John Doe</td>
<td>100</td>
<td>3.4</td>
</tr>
<tr>
<td>3 last name with model name</td>
<td>Doe’s MacBook Pro</td>
<td>47</td>
<td>1.6</td>
</tr>
<tr>
<td>4 last name</td>
<td>Doe</td>
<td>19</td>
<td>0.6</td>
</tr>
<tr>
<td>5 first name with model name</td>
<td>John’s MacBook Pro</td>
<td>753</td>
<td>25.5</td>
</tr>
<tr>
<td>6 first name</td>
<td>John</td>
<td>399</td>
<td>13.5</td>
</tr>
<tr>
<td>7 alias with model name</td>
<td>Gandalf’s MacBook Pro</td>
<td>271</td>
<td>9.1</td>
</tr>
<tr>
<td>8 alias</td>
<td>Gandalf</td>
<td>719</td>
<td>24.3</td>
</tr>
<tr>
<td>9 model name</td>
<td>MacBook Pro</td>
<td>218</td>
<td>7.4</td>
</tr>
<tr>
<td>10 miscellaneous/random</td>
<td>iBR7tvf9Bg</td>
<td>11</td>
<td>0.4</td>
</tr>
</tbody>
</table>

acquaintance for whatever purpose. If Bob wants to know who Alice is meeting regularly, he could infer her social relations by monitoring the network over a period of time to identify correlations of device names in data samples including Alice at different points in time. Location privacy and the involved issue of user tracking is a prominent privacy issue that has attracted considerable attention in recent years [370]. One common approach to track users is to follow the unique MAC address of their Wi-Fi devices [275, 269]. While the MAC address does not directly allow identification of a user, the device name in mDNS messages sent by the same MAC address facilitates matching of a captured track to a particular person. Once device and identity have been linked, individual behavior profiles can be created. If an attacker has enough resources to track Alice over a longer time period and at different locations, he can easily build a detailed behavior profile containing information about how long she stays at work, when she leaves home, is at the cafe, or goes to the gym.

The fact that Zeroconf protocols are not only announcing details about software services but also about existing hardware services (e.g., printers, scanners, cameras) allows attackers to easily build inventory lists of users. Especially, when the device name itself contains the type of device (e.g., AirPrint Canon iP3600 series @ Alice-Doe’s-MacBook-Air._ipp._tcp.local), as was the case in 58% of all analyzed mDNS messages in our dataset. If an attacker receives such an announcement in the cafe, he knows not only that Alice has a MacBook Air but also a Canon iP3600 printer at home. With the already deployed tracking system, the attacker knows the best time to burglarize Alice’s home.
3.4.3 Study: Privacy implications of presence sharing

Mobile messaging applications have emerged as mostly free alternatives to conventional SMS messaging on smartphones. WhatsApp is one of the most popular applications of that type with more than 500 million users [368] and more than 20 billion messages sent per day in 2014 [306]. Mobile messaging applications commonly support sharing of presence information, which communicates a user’s online status to others (e.g., being online, busy, offline), whether the user is typing, or if a particular message has been read by the recipient. While conventional desktop messaging applications, such as Skype or Jabber, typically rely on users manually selecting their presence status, most mobile messaging applications automatically infer the presence information from user interactions. For example, WhatsApp automatically sets the presence status to “online” when the application is in the foreground, and to “offline” when it is put in the background. A “last seen” timestamp further reports when a user was last online. The user’s presence status and “last seen” timestamp can be seen by any other WhatsApp user as long as the phone number is known and was added to the phone’s address book. While the “last seen” timestamp can be deactivated by users, the automatic transmission of the presence status (i.e., online or offline) cannot be deactivated.

Automated interaction-triggered status updates combined with the fact that mobile messengers are often used throughout the whole day make the resulting presence information potentially much more privacy sensitive than similar presence information in desktop messaging applications. In a collaborative work with Buchenscheit et al. [15], we investigated the privacy implications of presence sharing in such mobile messaging applications by collecting and analyzing presence information (i.e., the online status) of two independent groups of WhatsApp users over a four week. We based our investigations on WhatsApp, as we were able to collect presence information of WhatsApp users by exploiting a design flaw in the WhatsApp protocol.

Methodology

We recruited two independent groups of 10 (6 female, 17-29 years) and 9 (6 female, 20-28 years) WhatsApp users from a student population. After we obtained their initial consent, we collected their presence information over a four week period of regular WhatsApp use, resulting in over 27,000 presence updates and reflecting 545 hours of WhatsApp use in total. We took particular care to prevent priming participants about privacy in order to avoid influencing their WhatsApp usage behavior. We opted for a deception study design in which participants provided their phone number and consent to “collect us-

4 The author primarily guided the study design and conducted the analysis of potential privacy risk.
3.4 PRIVACY IMPLICATIONS OF UBICOMP

Figure 3.3: Presence information showing the WhatsApp activity of group 1 during one day. Tagged examples show that presence information can reveal wake up and sleep times, daily routines, and even conversation partners.

age information everybody else could collect as well” without being aware of what specific data we collect.

After the data-collection phase, we conducted semi-structured interviews to obtain a ground truth for participants’ behavior, such as sleeping hours or typical activities, as well as behavior at specific occasions identified in the collected data. In order to investigate participants’ awareness and perceived privacy concerns, we showed participants a visualization of their own presence information in relation to the anonymized presence information of other participants in their group. Each participant received a full debriefing detailing what data was collected, what we learned from it, and for what purpose the data would be used (anonymized data analysis and use in research publications). After the debriefing participants could freely choose to explicitly affirm or withdraw their consent. All participants consented to the use of their data in our research.

Results: Privacy risks

We visualized the collected presence information to ease the identification of potential behavior patterns and privacy implications. Figure 3.3 shows this visualization for a complete day of the first group. For each participant (rows) a bar on the time-line represents a period of active WhatsApp usage. Each use period is defined by a pair of corresponding available/unavailable events. While the visualization allows to see when participants were actively using WhatsApp, we were interested in further information that could be extracted from this data. Thus, in addition to calculating usage statistics we investigated the feasibility of inferring daily routines (e.g., bedtimes or working hours), as well as communication partners.

WhatsApp Usage The collected presence information reveals a detailed picture of a user’s WhatsApp behavior (e.g., time of uses, number of uses, or usage time per day). This information could lead
to several privacy implications. For instance, a superior could check whether employees are excessively using WhatsApp on workdays. Even more problematic is the particular time of use. In institutions that prohibit use of personal mobile devices during work or school hours, superiors or teachers could easily detect when policies have been violated. Ten participants (5 in each group) reported that they regularly use WhatsApp at work even though personal phone use is prohibited. Based on their presence information charts, three participants (P5, P6, and P9) specifically identified their WhatsApp usage during work and school hours in violation of respective policies. Seven of them stated that their phone number is known to their superiors, which would allow them to collect the required presence information and detect the policy violation.

**Daily Routines** Our visualizations of presence information suggest that patterns may reveal participants’ daily routines, such as bedtimes, working hours and variations thereof. We calculated average wake up and sleep times for the complete 4 week datasets and compared those to times reported by participants in the exit interviews. Estimated bedtimes were based on the first event in the morning after a longer pause and the last event in the evening or at night followed by a longer pause.

While the results exhibit some deviation (between 11 and 91 minutes, details are provided in [15]), they largely reflect participants’ stated behavior. More accurate results were achieved for participants who stated to usually check for new WhatsApp messages in the morning directly after getting up (16 participants) and regularly before going to bed (8 participants). One participant (P4) even stated that he always checks WhatsApp when waking up during nights (e.g., to use the restroom). Thus, monitoring of bedtimes and variations thereof could be used to assess the productivity of employees or students. Someone who regularly goes to bed at 10pm is presumably more well rested and productive than someone who is partying until 4am twice a week.

The collected usage statistics further allow to identify deviations from daily routines, e.g., longer usage at nights or unusually long pauses during the day. Recurring variations, e.g., long pauses at particular days of the week led us to assume that participants performed weekly activities in which mobile devices could not be used, e.g., during sports or rehearsals. In the exit interviews participants were asked to explain variations in their usage patterns of the last week before the interviews.

All participants were impressed how well their activities could be depicted: “Yes, here I was out at Saturday night [. . . ] here you see how long I went to the gym on Tuesday and that I played Basketball on Wednesday” (P1), “Friday I was bar-hopping till 5 am” (P2), “here you can see my
Figure 3.4: Conversation probabilities for P10 with other participants of group 1 during the complete period of data collection. Probabilities were calculated for one hour time windows. Almost all probable conversations were confirmed in the exit interviews.

afternoon nap and on Saturday our work party” (P3), “yes, on Friday I was out till 3:46am” (P4), and “here I was skiing and had no network connection” (P5). Participant P4 further stated that she was on vacation in a different country for a weekend, which was clearly revealed by an irregular long pause compared to her usually intensive WhatsApp usage. All participants of the second group confirmed their attendance of a student party on Wednesday night, which was clearly visible by many presence information events of 8 participants after 1am on a usual week day.

While the correct inference of activities often depends on the usage frequency and further context knowledge about a person (e.g., hobbies or profession), our results highlight the feasibility of automatically detecting daily routines and their variations, which could have several privacy implications. For instance, knowing that someone usually does sports on Wednesdays and is not using messaging applications during this time, it is trivial to observe whether this person is exercising regularly or not (e.g., when no pause of messaging activity occurred).

COMMUNICATION PARTNERS One of the most concerning findings was the ability to identify communication partners based on their presence information. While it was even possible to manually identify likely conversations from the visualization of presence information (see Figure 3.3), we also employed methods from social network analysis [298] to determine potential communication partners.

We calculated conversation probabilities between all participants of each group for the complete data collection period. The probability is the ratio of the summarized duration of overlapping presence information events to the total duration of the specified time period. Probabilities were calculated for one hour time periods. Figure 3.4 shows the conversation probabilities of P10 as an example. Peaks indicate hours with high conversation probabilities between two participants. Seven of the twelve depicted probable conversations were confirmed in the interviews.
While overlap in app use is a relatively naive proxy for a conversation, this approach is already sufficient to automatically identify bursty and focused conversations [696]. In the four week dataset of the first group, we identified 13 conversations which have been confirmed by the respective communication partners in the exit interviews. For the second group we could not identify any obvious conversations, which could be caused by the fact that participants of that group exhibited weaker social ties.

Social, economical, or political motivations for revealing conversation partners can be manifold, e.g., reaching from a spouse’s jealousy to industrial espionage.

**Results: user reactions**

All participants stated to be aware of the online status and the “last seen” features and to know how they work (i.e., that someone who is shown as online is currently using the app and the timestamp shows the last time the user was online). For instance, P1 stated to regularly use the feature: “Sure, if you are waiting for an urgent answer by someone who is not replying but is shown as “online” in WhatsApp.” Most (17) participants had the “last seen” feature switched on and used it to monitor others’ last seen timestamps when waiting for a response (16), to check their bedtimes (6), or to check how long they stayed at a party or an event (8). However, six participants were not aware that the “last seen” feature could be deactivated.

When we confronted participants with the visualization of their presence information and our results of the analysis, most of them (13) were surprised or even shocked (6) by the feasibility of our automated collection, e.g., P6 stated “I’m really shocked that you could do this. I thought only WhatsApp would be able to do so.” Further, one of the two participants who deactivated the “last seen” feature wondered: “How is it possible for you to get this data although I have deactivated the feature?” (P10) This highlights that users might not be aware that deactivating the “last seen” feature does not affect the sharing of the current online status, which cannot be deactivated.

**Discussion**

Through our analysis of the captured dataset of 19 WhatsApp users for a period of four weeks, we identified several privacy risks stemming from presence information. While the online status and last seen timestamp are only updated each time WhatsApp is in the foreground on the phone and actively used, it accurately reflects a user’s interaction with the app.

Our results show that presence information allows to create detailed usage statistics (i.e., when and how long someone is using WhatsApp), to derive a user’s daily routines (e.g., bedtimes, work
hours or school hours), and even to infer communication partners with sufficient reliability. Social or even economic and political implications of misusing such information are manifold. Privacy implications become particularly prevalent in relationships with asymmetric dependency or power relations. As our results suggest, users are often not aware of potential privacy risks. While our data collection and analysis was focused on presence information of WhatsApp, our results are also relevant for other mobile messaging applications.

While the “last seen” feature can be deactivated by WhatsApp users, sharing the current online status cannot be deactivated and thus allows continuous monitoring. However, as shown in the interviews, users might not be aware that sharing the online status is not affected by deactivating the “last seen” feature. Thus, mobile messaging applications should provide clear and unambiguous privacy settings that allow users to disable the sharing of presence information for all or specific contacts.

Furthermore, we found that presence information can be requested by everyone for any WhatsApp user if the phone number is known. WhatsApp and other mobile messengers leverage the user’s phone number as an identifier to enable message exchange without prior exchange of contact requests. However, presence information should only be available to a user’s contacts to prevent abuse by third parties. This could be achieved by requiring mutual acceptance as contacts before messages can be exchanged. A potential solution would be to enable message exchange without prior establishment of a contact relationship but only provide access to presence updates once a bidirectional message exchange occurred.

3.5 PRIVACY ENHANCING TECHNOLOGIES

The privacy principles and legal frameworks discussed in Section 3.3 have influenced the development of several privacy-enhancing technologies. However, their focus on information privacy limits the impact of existing privacy-enhancing technologies to privacy implications of observations, see Figure 3.5. Enhancing privacy with respect to disturbances has not been the focus of existing privacy research. However, existing approaches in the research domain of interruption management could also contribute to the minimization of privacy-affecting disturbances.

In the following, we briefly describe PETs with focus on data minimization and anonymization, and with a particular focus on enhancing privacy in UbiComp applications. We further discuss existing approaches to minimize disturbances. Note that further related work will be discussed in the respective sections of our framework for user-centered privacy awareness and control in Part II.
privacy principles & legislation

privacy architectures for UbiComp

data minimization & anonymization

observations (information privacy related)

minimizing disturbances

disturbances

Figure 3.5: Existing privacy-enhancing technologies and related work on interruption management which could enhance territorial privacy in UbiComp with respect to observations and disturbances.

3.5.1 Data minimization & anonymization

Existing privacy research (especially on communication technology) often focus on enforcement mechanisms for information privacy at the system level without user involvement [245, 203]. The goal of such privacy-by-architecture [615] approaches is to reduce information privacy implications through data minimization and anonymization techniques. On the one hand, privacy should be protected by sharing personal data only at the detail level required for the operation of a service. On the other hand, anonymization techniques should enhance privacy through disconnecting personal data from the owner’s identity. Pfitzmann and Hansen [516] provide a good overview of related techniques by clarifying the related terms of anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. Spiekermann and Cranor [615] further discuss the relation of identifiability and linkability to different system characteristics as part of their framework for privacy-friendly system design.

In the context of UbiComp systems, data minimization and anonymization approaches have been extensively proposed to enhance location privacy [199, 370, 684]. A prominent example is the concept of mix zones and anonymity sets by Beresford and Stajano [91]. Instead of using unique identifiers for communication modules they propose to use changing pseudonyms in order to prevent the tracking of users. Gruteser and Grunwald [274] applied the concept of k-anonymity to location privacy. Instead of pseudonymously sharing the exact location, a region containing $k - 1$ other users is shared. This way k-anonymity guarantees that each released location information cannot be distinguished from information of at least $k - 1$ other users. The larger the value of $k$, the greater the implied privacy since no in-
Individual can be identified through linking attacks with probability exceeding $1/k$. However, the concept of $k$-anonymity has also been criticized for not ensuring privacy in any situation [407].

Duckham and Kulik [198] suggest to decrease the accuracy of location information to the minimum required by a service (e.g., provide only the street or city instead of coordinates). Myles et al. [465] propose to use a central location server to manage access control and obfuscation techniques for location queries of applications. They extend the P3P policy language [169] to respect privacy preferences at the user level.

Similar data minimization and anonymization techniques (e.g., obfuscation and blanking approaches) have been proposed for video-based monitoring or surveillance systems based on the detection of sensitive regions through computer vision algorithms [694]. Most detection approaches are based on motion or face-recognition techniques. But also visual markers, such as a colored cap or vest, have been investigated to identify sensitive regions [570]. While blanking techniques completely remove sensitive regions, obfuscation techniques pixelize or blur regions to prevent identification of persons but still enable the observation of their behavior [150, 689]. Such techniques can be combined with encryption schemes to allow access to raw video data only by authorized persons in case of emergency or court order as proposed by Senior et al. [582]. Templeman et al. [639] propose to recognize sensitive spaces (e.g., bathroom or bedroom) to prevent involuntary sharing of sensitive images by wearable life-logging cameras. Moncrieff et al. [459] propose to use contextual information (motion, common paths, and crowd size) to apply different data hiding techniques to a video surveillance system.

A first step towards supporting control of video surveillance at user level was made by Brassil [112]. He suggests to use a privacy-enabling device, which periodically sends a user’s location and a timestamp to a central “clearinghouse”. Privacy-aware surveillance systems query the clearinghouse for potential users who were in a camera’s field of view before publishing a video and obfuscate respective regions if necessary.

In contrast to those optimistic privacy control solutions for video systems, Truong et al. [652] propose a pessimistic approach based on detecting retro-reflective CCD or CMOS camera lenses. Once a camera is detected, a pulsing light is emitted towards the lens in order to distort camera recordings. The CamoFlash [289] and noPhoto [484] projects are based on a similar idea.

While the previous approaches only focus on the control aspects of privacy, Winkler and Rinner [693] aim to support awareness about video surveillance. As a discovery mechanism, they propose to combine a community-based approach for camera registration with extended privacy-aware cameras. The cameras allow users to query
meta information (e.g., about the operator, the purpose of use, or applied obfuscation techniques) by holding a dynamically generated QR-code in the camera’s field of view. This meta information can be additionally signed by a trusted third party in order to enable attestation of provided information.

Neustaedter and Greenberg [473] support both awareness and control in their context-aware home media space. Users were able to control a video communication system (e.g., by switching it off, setting the blur level or video resolution) and to receive audio-visual feedback in order to assess their current privacy level in the video system. They discuss their explicit and implicit control strategies in relation to Altman’s [45] social privacy regulation theory (see Section 3.2.3).

Christin [154] provides a good overview of related data minimization and anonymization techniques to enhance privacy in mobile participatory sensing applications.

3.5.2 Minimizing disturbances

As highlighted by the approaches for data minimization and anonymization, existing privacy-enhancing technologies of this domain only focus on the information privacy dimension, i.e., they address privacy-affecting observations (see Section 3.2.3). The territorial privacy dimension and the related impact on privacy by undesired disturbances has not been addressed by most existing research on PETs. An exception is the Mobile People Architecture (MPA) by Roussopoulos et al. [550], which aims at maintaining the reachability of persons. It is realized by a personal proxy that tracks a user’s location and handles incoming communications based on the user’s preferences. One claimed goal of the system is to preserve the privacy of a user by hiding all visited locations and by filtering incoming communications according to their desirability, as “receiving unwanted messages is also an invasion of privacy” [550].

Several other approaches exist that try to mitigate undesired interruptions by technological mechanisms even though not focusing on privacy. Nevertheless, those approaches could contribute to the design and development of solutions for enhancing territorial privacy.

A common approach to mitigate disturbances is to provide others with context information about one’s own situation or availability for interruptions. An early attempt to realize this for desktop and mobile devices was made by Tang et al. [637]. They propose to share information about the online status, the used input device (e.g., keyboard or mouse), the engagement in any computer-mediated communication, the current location, and appointment schedules. The context information is presented to other users as meta information attached to a contact list in order to support contacting decisions. Similar approaches on mobile devices have been already discussed in Sec-
While those approaches could decrease undesired privacy-affecting disturbances on the one hand, they create potential privacy-affecting observations through sharing of context information on the other hand. Birnholtz et al. [100] tried to address this issue in their OpenMessenger system for online communication through the idea of *gradual initiation* of interactions. Context information can be shared on different levels and users get notified whenever information is accessed by others in order to enhance the negotiation of interactions similar to real world face-to-face interactions (e.g., in office environments). However, the visual and auditory notifications proposed by the authors could also be perceived as undesired disturbances, which was also confirmed by the results of their preliminary evaluation.

Instead of letting users decide on the appropriateness of an interaction or the availability of a person, other approaches try to create models for supporting automatic recognition of a person’s availability and interruptibility. Kern et al. [351] propose a model of human interruptibility which distinguishes between the two axis of *personal* and *social interruptibility*, that is interruptibility of the user and interruptibility of the environment. The latter refers to the interruptibility of persons in the environment, which should be respected, e.g., to mitigate embarrassing situations such as a ringing phone in a lecture. For both forms they define the interruptibility as a continuous value ranging from *don’t disturb*, over *interruption ok*, to *interruption no problem*. Based on this model they implemented a prototype that automatically recognizes the current interruptibility by wearable sensors and maps it on an appropriate notification intensity [352]. The three notification intensities (don’t notify, make aware, and grab entire attention) are realized through different modalities, e.g., vibration, a beep, or a ring-tone.

Ho and Intille [304] use wireless accelerometers to detect moments of activity-transitions that are best suited for delivering notifications. In a similar manner Horvitz et al. [310] propose methods for inferring the cost of interruptions by notifications. In addition to sensor data, they leverage information about a user’s interactions with devices and calendar data to determine the expected cost of an interruption.

Also Fogarty et al. [232] investigated sensor-based statistical models of human interruptibility. They demonstrate that such predictive models could provide reliable results in office environments. In a subsequent work [233] they extend this approach to automatically share information about a user’s availability detected through the microphone of a user’s laptop.

Existing approaches to minimize interruptions show that facilitating observations can help to reduce disturbances. This confirms that from a privacy point of view observations and disturbances (see Section 3.2.4) are strongly interrelated and should be respected in conjunction when designing user-centered privacy solutions in UbiComp.
3.5.3 Privacy architectures for UbiComp

Langheinrich [388] adapted the fair information principles (see Section 3.3) to UbiComp scenarios and followed those principles to design the privacy awareness system PawS [389]. PawS addresses information privacy issues stemming from third party data collection in smart environments. The system is based on privacy policies, privacy proxies, a privacy database, and a personal privacy assistant. Privacy policies contain the data handling practices of services in a user’s environment. They are either implicitly announced via service discovery protocols or explicitly via so-called privacy beacons. Privacy beacons are wireless broadcast messages transmitted in the affected physical proximity of a UbiComp service (e.g., a monitoring system). It is assumed that personal data is managed by a personal privacy proxy and all UbiComp services provide a service proxy. The personal privacy proxy controls all third party access to personal data by comparing collected policies with a user’s predefined privacy preferences. When access is granted, the shared data and associated policy is stored in a central privacy database. The privacy assistant keeps track of all policy announcements and data collections by UbiComp services. While PawS allows awareness and control of information privacy in UbiComp, the assumptions of a central privacy database and privacy proxies hamper the efficient realization of this approach for complex UbiComp scenarios with many decentralized services that typically store and forward data without respecting central components.

Confab is a similar proxy-based privacy-aware architecture for UbiComp proposed by Hong and Landay [305]. Confab is based on the concept of information spaces [331, 330]. Information spaces organize objects (i.e., information, resources, and services) and can be delimited by physical, social, or activity-based boundaries, which is motivated by social privacy regulation strategies (see Section 3.2.2). Confab combines such information spaces with in- and out-filters to manage the flow of personal information. Similar to the concept of sticky policies [462], so-called privacy tags can be attached to information when flowing outside of an information space. Privacy tags describe personal privacy preferences, e.g., when information should be deleted (control) or that the owner should be notified when the information is accessed (awareness). Similar to PawS, the enforcement of those preferences depends on a trusted runtime environment. The confab architecture is further extended by Price et al. [521] and combined with a personal digital rights management (PDRM) approach as proposed by Gunter et al. [278].

Kapadia et al. [342] use a similar metaphor of privacy boundary regulation (see Section 3.2.2) and propose a privacy policy language based on the concept of virtual walls. The policy language allows to set three transparency levels similar to physical walls in order to control
the access to personal information: transparent (full virtual access), translucent (anonymous or obfuscated virtual access), and opaque (access limited to physical boundaries). To enforce such policies a trusted context server is required, which handles the access control and setting of virtual walls similar to the proxies in PawS [389] and Confab [305]. Pan et al. [499] built upon the idea of virtual walls and provide a location estimation approach based on received signal strength (RSS) values from mobile clients in order to allow access control within user-defined digital boundaries. Also Takeuchi [636] uses the metaphor of virtual walls to limit the interruption of noise in an open office environment through the use of noise-cancelling headphones.

Another metaphor from social privacy theory is leveraged by Lederer et al. [395]. They propose the metaphor of faces to support the control of personal privacy in terms of with whom, what, and when information is shared. Awareness of privacy implications is supported by an accessible log showing past disclosures. While users were free to define individual faces with different privacy preferences, the results of a user study revealed that it was difficult for them to remember their settings of faces. These insights lead to the identification of the five pitfalls for designers of privacy technologies in UbiComp as discussed in Section 3.3.

Moncrieff et al. [460] applied their idea of context-aware privacy in video surveillance [459] to a multimodal sensing scenario of a smart home safety system. Their goal is to support the dynamic regulation of privacy boundaries due to changing context in different situations (see Section 3.2.3). They distinguish between spatial context (i.e., the current location), social context (i.e., interactions between persons or third parties), hazardous context (i.e., abnormal interactions with hazardous devices), and temporal context (i.e., abnormal periods of inactivity). Context information is gathered by several binary and audio sensors and mapped to appropriate privacy policies based on a decision tree. The mapping process is further influenced by the purpose of data access (e.g., diagnostic aid by a doctor), the trust level in the entity accessing the data, and the currently assumed thread-benefit trade-off. Policies are enforced by providing access to audio, video, and binary sensor data, in five different granularity levels similar to the data minimization techniques discussed in the former section. Moncrieff et al. suggest to provide privacy awareness about the currently accessible granularity level by different colors of an ambient light, e.g., the Ambient Orb [46].

Tentori et al. [641] introduce the concept of quality of privacy (QoP) in the context of pervasive healthcare. The term QoP basically reflects similar granularity levels (low, intermediate, high) as described by Moncrieff et al. [460]. Those granularity levels are defined by users in their privacy preferences and by service providers in their privacy
policies in order to allow the negotiation of a privacy contract similar to the process in Langheinrich’s [389] PawS architecture. The enforcement of a privacy contract is provided by autonomous agents, which have been implemented as an extension to the Simple Agent Library for Smart Ambients (SALSA) middleware [541]. Similar to Moncrieff et al. [460] they propose to use context in order to automatically select the appropriate QoP level, e.g., based on a user’s location, the current time, or the presence of other persons.

3.6 SUMMARY

Even though privacy is a well-known concept, it is associated with many different expectations, values, as well as informational and physical dimensions. The different theoretical frameworks and models discussed highlight the individual and dynamic nature of privacy in everyday situations. Our concept of territorial privacy is based on those different theoretical backgrounds and covers aspects of information privacy as well as physical privacy aspects related to the invasion of personal space or undesired disturbances.

While the dimension of information privacy has long been the focus on privacy research in the online world, our discussion of privacy implications in UbiComp shows that also the physical aspects of territorial privacy become much more important in UbiComp systems again. The context-awareness of those systems relies on gathering and processing a multitude of information about users and their environments, which in many cases happens invisible due to the embedded and unobtrusive nature of UbiComp systems. This leads to the fact that users often are not aware of potential privacy implications. The often involved context-based actuation and interaction capabilities can further cause disturbances by undesired interventions in a user’s environment. Furthermore, the ubiquitous inter-connectivity of devices and services makes it hard for users to determine the shifting virtual boundaries of their privacy. These UbiComp characteristics can cause many undesired observations and disturbances, which are reflected in our concept of territorial privacy.

Existing privacy principles and legislation provide meaningful basic requirements, which need to be respected when developing technical solutions. Those requirements can be categorized in awareness and control principles at the user level and enforcement principles that support the implementation of awareness and control at the system level (see Figure 3.1). We respected these principles in the development process of our user-centered privacy framework.

The discussion of existing privacy-enhancing technologies showed that most work is focusing on the informational privacy dimension by providing solutions for data minimization and anonymization. While research on minimizing disturbances exists in the domain of
interruption management, these approaches are not directly related to privacy but nevertheless can support the development of privacy-enhancing technologies with the goal of mitigating privacy-affecting disturbances. While we can see that the privacy dimensions of observations and disturbances are often interrelated, especially in UbiComp scenarios, no research exists that addresses both dimensions in conjunction. In general the physical aspects of territorial privacy have been neglected by most privacy research in UbiComp.

As shown by our discussion of related work on users’ awareness of technological privacy implications and also by our own studies of ZeroConf and WhatsApp, awareness of privacy implications stemming from prevalent technologies is already an issue today. The identification of potential privacy implications will become even harder for invisible UbiComp technology.

Providing better awareness of technological processes and systems’ purposes would not only prevent misconceptions and falsely perceived privacy implications, but could also support users in making more informed decisions about privacy control. Furthermore, providing privacy awareness has the potential to help users in better aligning their mental models of perceived privacy implications to the real implications stemming from underlying system models.

In order to identify the relevant factors of privacy awareness and control at the user level, we review existing user studies that investigated users’ privacy concerns at the context of UbiComp applications.
In order to understand user needs and concerns about privacy in UbiComp we did an extensive literature review of existing user studies in this domain. We further discuss the results of our own studies in relation to existing work. The results of this review and of our own studies guided the development of our territorial privacy model.

Relevant literature can be broadly categorized into studies that investigate general privacy concerns, privacy in location sharing, privacy on mobile devices, and privacy in smart environments. Even though the last category promises to be most related to UbiComp, the findings of all categories are relevant in order to understand the broad landscape of privacy issues in this context and to identify requirements for privacy protection mechanisms from a user’s perspective. We discuss how those findings relate to territorial privacy (see Section 3.2.1) and how they support the development of concepts for awareness and control of privacy in UbiComp.

The used methodologies for studying privacy concerns range from surveys and focus groups to experiments and case studies. Some researches [75, 313] argue that studying privacy is most valuable when it is conducted in real-world situations (e.g., explored through case studies or experiments) because participants’ answers in surveys or interviews often do not match their actual behavior in practice [616, 329]. While this is a reasonable concern, studying privacy in UbiComp in real-world situations is especially challenging as most UbiComp systems do not yet exist in real world. An often applied compromise is the use of scenario-driven surveys and interviews to increase the reliability of gathered answers [313].

4.1 GENERAL PRIVACY CONCERNS

Between 1978 and 2004, Alan Westin extensively studied people’s general privacy concerns in the US by conducting over 30 different representative surveys [373]. For most of them he created a privacy index to categorize the population into privacy unconcerned, privacy pragmatists, or privacy fundamentalists. The results of his surveys showed that till 2003 most people were privacy pragmatists (64%) “who have strong feelings about privacy and are very concerned to protect themselves from the abuse or misuse of their personal information by companies or government agencies” [638]. However, as Westin’s privacy index relies on broad self-reported privacy attitudes, their predictive power of a per-
son’s behavioral intent or reaction to specific consequences in privacy-affecting situations remains questionable [616, 697].

Westin’s surveys did also investigate the relevance of different privacy dimensions (see Section 3.2.1), showing that information privacy aspects were extremely important for most persons (79%) (e.g., being in control of who can get information). But also territorial privacy aspects gained significant importance between 1994 and 2003, e.g., not being disturbed at home (extremely important for 49% in 1994 and for 62% in 2003), and being able to have times of being completely alone, away from anyone else (extremely important for 54% in 1994 and for 60% in 2003). Similar results were reported by the EU’s large-scale study on European citizen’s behaviors and attitudes concerning privacy in 2011 [647]. Information privacy was of high importance for 75% of Europeans (e.g., being able to delete personal information from websites, and approving any kind of personal information collection or processing). About 70% were concerned that companies use their personal information for other purposes than specified during collection. Regarding territorial privacy, about 40% worried about being recorded in private spaces (e.g., restaurant or office) and 34% worried about being recorded in public spaces (e.g., subway or airport).

The importance of those different privacy dimensions could also be influenced by age as suggested by the results of focus group interviews conducted by Kwasney et al. [376] in 2008. They found that younger adults had a much broader conceptualization of information privacy whereas older adults were more concerned about territorial privacy aspects. This could be caused by the fact that younger adults are much more engaged in information technology usage. While Hoofnagle et al. [307] did not find any differences between younger and older adults’ attitudes towards information privacy online, they found that younger adults often had less knowledge of privacy law, which could be a reason for their more unconcerned engagement with online services.

General privacy concerns have also been investigated related to different environments, e.g., at home or at work. Marshall [437] studied how features of the physical environment influence territorial privacy expectations at home. They found that low perceived privacy at home was primarily influenced by the number of rooms per person, the ability to insulate noisy and quiet activities from each other as well as noise of, distance from, and visibility of neighbors. Similar findings have been reported by Takami and Teeravarunyoo [634] who investigated the territorial privacy implications of small shared apartments common in many Asian countries. Pedersen et al. [512, 511] found that also the sound and visibility of near-by wind turbines are sometimes perceived as a privacy intrusions for people with high expectations of peace and quietness at home.
De Veer and Kerkstra [184] investigated factors influencing feeling at home with respect to privacy in nursing homes. They found that perceived attitudes of nurses and perceived disturbances by other residents significantly influenced feeling at home. Similar territorial privacy aspects have also been studied for patients in hospitals. Grumet [273] found that privacy is often disturbed by noise made by other patients or nurses. Also Sawada et al. [567] found that nurses often did not respect the personal and territorial space of patients by making noise or turning the lights on.

Regarding office environments, several studies [118, 181, 99, 193] have shown that open-plan offices reduce employee’s satisfaction and perceived privacy, especially in terms of visual and acoustical privacy [193]. Birnholtz et al. [99] explored privacy factors in open-plan offices to gain insights for the privacy-aware design of distributed collaboration and awareness systems. They found that attention is an important factor influencing territorial privacy aspects related to the initiation and management of interactions. While indicating paid attention is required for signaling the willingness for interactions, this must be done in a noninvasive manner in order to reduce undesired interruptions.

While interruptions in general could cause disturbances and therefore perceived privacy violations, they have been studied in literature typically without privacy considerations and mostly in focus of relations to task execution and productivity. However, findings could nevertheless contribute to the understanding of privacy violations through disturbances in UbiComp.

Carton and Aiello [136] found that the negative effects of undesired social interruptions (e.g., by conversations) on stress and task performance can be lowered by providing awareness of potential interruptions and supporting control of undesired interruptions.

Harr and Kaptelinin [287] investigated social context used by people when making decisions about interrupting other persons. They identified the interpersonal relation, a person’s location, and the knowledge about whether or not the person is involved in a communication or collaboration, as the most relevant social context influencing interruption decisions. The same context factors have been found important from an interruptee’s point of view in order to accept or reject potential interruptions [713, 229]. Zulkernain et al. [713] did further identify the interruptee’s schedule, the interaction history with the interrupter, and the interruption content as relevant decisive factors. Fischer [229] does also discuss these factors in his Contextual Factors of Interruptions (CFI) Model and extends relevant interruption properties by the medium, presentation, and timing of an interruption.

Warnock et al. [680, 679] studied the disruptiveness and effectiveness of different modalities (e.g., visual, auditory, or tactile presentation) for notifications. They found that modality had no effect on error
and success rates of performed tasks, but unwanted notifications had a negative effect on task performance, highlighting the need to avoid such notifications. Adamczyk and Bailey [32] showed that the timing of interruption during different task executions had an impact on a person’s emotional state and positive social attribution.

The findings of the discussed studies highlight the importance of territorial privacy aspects in everyday life. With respect to privacy in UbiComp, users should be aware of potential disturbances and should further be able to avoid undesired disturbances. Outcomes of research on task interruption management can help to identify required factors for realizing awareness and control of privacy-affecting disturbances in UbiComp.

4.2 PRIVACY IN LOCATION SHARING

One of the first and still most valuable context factor used in UbiComp applications is the location of users (see Section 2.2.4). As the central information for location-based services and awareness-systems that allow sharing the own location with others, a user’s concern about providing the own location information has been investigated by many studies. Especially with the mass distribution of mobile devices and smartphones research in location privacy became a prominent topic [91, 199, 370]. Table 4.1 summarizes the factors that have been identified to influence privacy awareness and control in related user studies of location sharing applications. We discuss the results of these studies in the following.

In an experimental case study Barkhuus and Dey [74] examined location privacy concerns in relation to the use of location-based services. They found that an important factor influencing privacy concerns was how the location was collected and for what purpose it was used, e.g., for a position-aware service or location tracking. Also who was receiving the location influenced the perceived intrusiveness. Similar results were reported by Consolvo et al. [163] who found that in their social location sharing application it was most relevant for users who was requesting a location and why the location was requested (purpose). Further effects were identified by contextual factors, such as users’ current location, their current activity and mood. The time of a request influenced how disturbing a location request was perceived. Several users did not want to be disturbed by a request during “alone time” or a “private day.” Interestingly the granularity of a shared location was not perceived as a tool to control privacy. Participants shared the detail level of their location which they thought was the most useful for the recipient. Knijnenburg et al. [361] even argue that controlling granularity of location is not needed and can be compensated by other decision strategies of users. However, in a two month study conducted by Brush et al. [120], participants were
comfortable in mapping their privacy expectations on similar obfuscation techniques for their location, e.g., mixing, deleting data near home, and randomizing. Participants were further more willing to share their location anonymously and with trusted recipients.

The relationship to the recipient and its involved trust was reported as most influential be several other studies [50, 649, 653, 572, 88]. Therefore, many users prefer to control access to their location on group level [163, 649, 556, 653, 88], e.g., friends, family, or colleagues.

As already identified by Barkhuus et al. [74], how location information is collected and for what purpose it is used further influences privacy concerns of users. The meaning of the purpose of location sharing, i.e., why location is accessed by other persons or services was confirmed by several other studies [163, 507, 361]. In two user studies Schlegel et al. [572] also found that perceived privacy concerns are influenced by the frequency of access to location information, which aligns to the findings of Barkhuus et al. [74].

Table 4.1: Main factors influencing privacy awareness (◦), privacy control (+), or both (⊕) in location sharing applications. While location privacy is an information-centric privacy issue, existing studies mostly reveal insights on the privacy implications of observations (⊿) and not on disturbances (◀).
Similar to Consolvo et al.'s work [163], other studies identified contextual factors influencing perceived privacy concerns and control decisions in location sharing. The current location (e.g., at home, at work) was found to be important for users in several other studies [50, 556, 649, 507]. Toch et al. [649] found that users were more comfortable in sharing their location at places with a large number of other persons. In addition to the current location, they investigated also the current time as a contextual factor influencing privacy concerns. Their results suggest that users want to be aware of when location information is accessed or requested by others, and that users are able to specify time based access control rules accordingly. Similar results have been reported by Tsai et al. [653] and Benisch et al. [88]. However, in a 3 week field trial of the Peoplefinder application, Sadeh et al. [556] found that people had a hard time expressing similar rules based on own location and time. Also the results of Patil et al.’s study [507] with free-form access rules specified in everyday language by more than 100 participants suggest that time-based constraints are less important and describing such rules is challenging for users. In addition to the former context factors, Anthony et al. [50] further identified the social context (alone or with others) as an important factor influencing the willingness to share location information. Their participants were more willing to share location information when they were alone.

While the former results only inform about users’ privacy concerns with respect to their location, similar findings have been reported for other sharing applications that in addition to the own location allow to share the own identity, profile, and activity [396], or to share availability and calendar information [506]. However, the location was often viewed as the most sensitive information [506] and users expressed the desire to configure their privacy preferences at the group level, e.g., for family or colleagues.

With respect to these studies, we can identify several factors that are required to support privacy awareness and control in location sharing applications. While the results of most studies provide insights to the information-centric privacy dimension, i.e., regarding privacy-affecting observations (see 3.2.1), the results of Consolvo et al. [163] also contribute to the physical dimension of privacy with respect to privacy-affecting disturbances.

As shown in Table 4.1, the influencing factors can be summarized in who has access to location information, to what location information (e.g., granularity), when it is accessed (i.e., under which context conditions), how it is accessed (e.g., the frequency of access), and finally why location information is accessed (i.e., the purpose of access).
With the widespread use of smartphones and similar personal mobile devices the use of location information by different mobile applications (apps) has become common practice. But not only the location of users matters to mobile apps. Through different sensors and rich personal information stored on such devices today, mobile apps can access a huge amount of sensitive information. Thus, on the one hand personal mobile devices pose a central risk for the information-centric privacy dimension with respect to observations. On the other side, personal mobile devices increase the availability of users for any kind of notifications, incoming calls, or messages. Thus, mobile devices also pose risks for the physical dimension of privacy regarding disturbances. Table 4.2 summarizes the influential factors for privacy concerns on mobile devices with respect to observations and disturbances, which are discussed in the following.

In a 3 week field study with 20 Android users, Jung et al. [333] found that users desire a better awareness of information flows in order to make more informed privacy decisions when installing new applications. Also awareness about the history of access to information was desired. Thompson et al. [646] showed that awareness about access history could even allow users to identify misbehavior of apps. But even if users would be aware of resource access and information flows, they still have a hard time in reasoning about the purpose of information access, as Lin et al. [409] point out. In a large scale online study they found that users are not able to guess the purpose of resource access by an application, and would rather explicitly be informed about it. Similar results have been reported by Balebako et al. [70]. Participants of their qualitative lab study requested more detailed information about who is accessing information, how frequently, and for what specific purpose. To better understand why applications required specific permissions was also an important desire of participants in Kelley et al.’s [350] study, highlighting the importance of awareness about the purpose of information access.

While the previous studies focused on privacy-affecting observations, the following also addressed aspects of disturbances in the context of interruption management on mobile devices. Toninelli et al. [651] studied the relevant factors users take into account when answering phone calls. The relationship to the caller and the own activity were found most important. Similar to Hudson’s and Smith’s [312] strategies for privacy and disruption tradeoffs, they propose to share context information (e.g., availability or location) with callers. Callers should then decide on the appropriateness of a call, which could potentially reduce undesired disturbances. For both cases, answering phone calls and sharing context information, they asked users to define respective control strategies. Interestingly, they found that users
tend to express similar strategies for both cases, which could be modeled as access control policies to a user’s resources (i.e., regulating access to a user’s context information on the one side, and to a user’s attention or availability on the other side). Similar access strategies have been observed for instant messaging users who regulated their privacy preferences regarding the “access to the self” through blocking strangers and configuring their connectivity status accordingly [272].

Based on these results Toninelli et al. [650] developed a usable policy model for mobile devices, which allows to express control preferences by who should have access to which resource, how access should be granted, and under which conditions (i.e., when, where, and why). Their results show that observations and disturbances can and should be modeled together to support a user’s privacy control decisions. While such policies would allow to filter phone calls automatically, participants did not want automatic filtering and preferred to decide when a call arrives. Mostly because deciding in advance was perceived as too difficult and users feared a lack of control.

Sharing context information with callers in order to avoid disturbances by phone calls has also been investigated in other studies [354, 362]. Khalil et al. [354] found that users were willing to share more detailed context information (e.g., their location and activity) with persons in closer social relation (e.g., family and friends). Also Knittel et al. [362] showed that group level control of sharing context information was highly accepted. Controlling the granularity of context information was another important aspect for users. Depending on the social relation with a respective group they shared different location details (e.g., only the city or the exact position). The former studies show that control of disturbances might depend on controlling observations, which in turn shows that both should be considered together with respect to privacy.

In contrast to let callees share their context information, Grandhi et al. [265] propose to let callers share more detailed information about the reason of a call based on their former findings of incoming call analysis [264, 262, 263]. While they found that the relationship with the caller was still the most influencing factor for call acceptance decisions, the influence of a call’s reason and importance was also very high. Similar findings have been discussed by Fischer et al. [230] for the perceived quality of interruptions by SMS. The relevance of the message’s content was much more influential than the time it arrived. These results show that the purpose of a disturbance needs to be respected as well to support privacy awareness and control.

Also the disturbing character of general notifications on mobile devices has been investigated [304, 591]. Ho and Intille [304] found that notifications were perceived as less disruptive when they occurred between different physical activities (e.g., between sitting and walking). Based on several other studies they identified eleven factors that
further influence how the interruption by a notification is perceived, i.a., the user’s activity, the utility of message, the user’s emotional state, the modality and frequency of an interruption, and the user’s social engagement. Also Rosenthal et al. [548] found that the preferred modality of notifications depends on the user’s activity and the source of notifications. A large-scale study of the perceived quality of 200 million notifications on smartphones by Shirazi et al. [591] revealed that notifications from system applications were perceived less valuable than notifications from messengers and calendars. Notifications were considered important when they informed about events, or were related to the user’s context or contacts.

While the discussed influence factors (see Table 4.2) are similar to the ones of location privacy concerns, most studies either focus on observations or on disturbances, or on aspects of awareness and control, separately. Only some results provide holistic insights such as the work by Toninelli et al. [651].

Table 4.2: Main factors influencing privacy awareness (●), privacy control (+), or both (⊕) on mobile devices. Studies reveal influencing factors for observations (⊿) as well as for disturbances (◀).
4.4 PRIVACY IN VIDEO AND RECORDING SYSTEMS

In the following, we discuss the influencing factors for privacy awareness and control in video and recording systems, which are summarized in Table 4.3.

Early work on privacy in smart environments often focused on privacy concerns about video recordings, as video cameras constitute one of the first ubiquitous and multi-purpose sensors allowing a diverse set of UbiComp applications. Boyle et al. [110] studied the effect of blur and pixelization filters at different obfuscation levels on users’ privacy concerns and awareness information gathered from video images. While their results suggest that the obfuscation levels of blur filters provide better balance between privacy and awareness information than pixel filters, they only examined typical office scenarios. A different result was reported by Korshunov et al. [367]. They found that pixelization filters provide the trade-off between privacy protection and intelligibility of activities in indoor video surveillance. Neustaedter et al. [474] evaluated similar video obfuscation techniques in a home-based video conferencing system. They found that video blurring of video and similar image masking techniques are not sufficient to decrease users’ privacy concerns, especially in situations with more sensitive and personal activities. Users feel not comfortable relying on those techniques and rather prefer more direct control, e.g., turning a camera off or rotating it. Based on those results they proposed a context-aware media space for the home providing feedback and control features [473].

Similar results have been found by Demiris et al. [187] who investigated different obfuscation techniques in the context of video-based monitoring applications for elderly. Even though results suggest that older adults’ privacy concerns can be decreased by shape extraction techniques and capturing only silhouette images of users, they still expressed the desire to switch the system off. They also were concerned about who would have access to the recorded images and would like to get informed when desired. Further control was desired in terms of frequency and location of the video monitoring system. The acceptance of such systems was highly influenced by its purpose and the perceived benefit for users.

Older adults’ privacy concerns of a monitoring systems with three different video processing approaches have also been studied by Caine et al. [128]. They found that concerns were influenced by the image type the device was capturing (blob tracker, point-light, or raw video) and the perceived benefit of the system, which depends on the users’ physical and mental condition. In a more recent work [127] they examined the influence of three different monitoring systems: a wall-mounted camera, a camera-equipped stationary robot, and a camera-equipped mobile robot. They found that older adults engage
Table 4.3: Main factors influencing privacy awareness (◦), privacy control (+), or both (⊕) in video and recording systems. Studies reveal insights on privacy-impacting observations (⊿), but not on disturbances (◀).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>who (recipient / source)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>perceived role</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>relationship with recipient</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>manual control</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>what (content)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>recorded information</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>granularity of information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>when (context)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>own location</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>own activity</td>
<td>o</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>time / history</td>
<td></td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>manual control</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>how (collected, disturbed)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>masking technique</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>recording technique</td>
<td>o</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aggregation technique</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>identifiability / anonymity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>access frequency</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>why (purpose, benefits)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>perceived purpose</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4.3: Main factors influencing privacy awareness (◦), privacy control (+), or both (⊕) in video and recording systems. Studies reveal insights on privacy-impacting observations (⊿), but not on disturbances (◀).

in “privacy-enhancing behaviors” while being monitored by those systems at home, e.g., covering the camera with an object, turning the camera in a different direction, or changing the own location. Interestingly those behaviors occurred more frequently with the wall-mounted camera than with robots. Unfortunately the reasons for this have not been investigated in this work. The own activity highly influenced the perceived privacy concerns. While sensitive or intimate activities increased concerns, being monitored in doing dangerous activities did not influence concerns, which shows that the perceived benefit of a monitoring system is also context-dependent.

These results highlight the diversity of privacy attitudes towards how video is recorded and processed and show that video recordings and applied privacy mechanisms need to respect individual preferences and contextual settings, e.g., the current activity of users and
environmental conditions. They further highlight that users should be made aware of applied filter techniques in order to assess the implied privacy risks.

The awareness of potential video recordings was also an important requirement for participants in Hayes et al.’s [291] long-term study of their BufferWare archiving system. At a specific location users could archive video- and audio-recordings of discussions and meetings. Users preferred visibility and transparency of any recording at this location in order make informed decisions. The way users wanted to be notified differed widely from notifications on every recording, receiving notifications only the first time, or no notifications at all.

Based on focus group studies, surveys, and interviews [33], Adams identified information sensitivity, information receiver, and information usage, as the key factors influencing privacy concerns in multimedia communication systems involving video and audio recordings [35]. The combination of these factors is utilized by users to evaluate a cost-benefit trade-off in form of a risk assessment.

Moving on from static to mobile scenarios of video recordings, Nguyen et al. [477] examined the perceptions and reactions of SenseCam, a wearable life logging camera for augmenting human memory with passive image recordings. Again participants wanted to be informed about when being recorded by someone else’s SenseCam and preferred giving their consent before any recording could take place. Furthermore, the purpose of a recording was of high relevance to participants and influenced their acceptance of potential recordings. In a similar study, Denning et al. [189] examined the reactions and concerns regarding augmented reality glasses. Participants’ concerns and acceptance of the recording were influenced by the place of recording, their current activity, who was wearing the device, and whether or not they were identifiable in the recorded data. Their participants further preferred to give their consent to any recording or have the ability to block recordings of augmented reality glasses in their environment.

Klasnja et al. [358] investigated privacy concerns of a wearable device that could infer a user’s physical activity based on four sensors: an accelerometer, barometer, GPS, and microphone. They found that concerns often depend on what is being sensed, in which context (e.g., location) it is sensed, and for what purpose. They conclude that the acceptance of an application is highly influenced by the perceived benefit and could be increased further by applying privacy preserving data handling practices, e.g., continuously purging raw audio and location data, or recording audio only in frequencies required for activity recognition.

Raij et al. [527] studied users’ concerns about the inference of personal habits (e.g., stress, conversation, smoking, or drug usage) by wearable sensors. They found that participants were only able to un-
derstand potential privacy risks when they had a personal connection to inferred information. While the type of information strongly influenced participants’ privacy concerns, their concerns were increased further when their identity or additional context was added to the information. They were most concerned about sharing the exact moments of stress or generally about sharing physical and temporal context together.

Denning et al. [188] explored patients privacy concerns about implantable medical devices with wireless capabilities. Their results suggest that patients are most worried about wearable devices that are connected to the implantable device (e.g., an alert bracelet and wristband) and would visually indicate their medical conditions to other persons. Furthermore, patients were concerned about alarm features that would also be noticeable by other persons and would require explanation. This highlights the need to respect also implicit privacy implications when designed such systems.

Massimi et al. [441] studied the understanding of general recordings in everyday environments, e.g., audio, video, pictures, or electronic tracks of computing activities. They found that people have different expectations and concerns about recording technologies in private, shared, and public environments (e.g., home vs. office vs. street). While most users accept recordings in public environments, recordings in private environments are mostly rejected. In shared and private environments the trust and relationship in people and in the space itself were found to be the most important factors influencing the presumption about recordings. According to Massimi et al. people tend to utilize externally observable features in order to assess public spaces with respect to the existence of recordings. For instance, the type of camera or recording device influences the presumption about what is recorded, for what purpose, and who has access to the recordings (e.g., a dome camera with tinted glass is associated with crime prevention, a similar but uncovered camera with other uses, such as traffic monitoring). Participants expressed that constant notifications about recordings would be desirable in crowded urban areas and shared or private spaces. However, in many other situations they preferred only single notifications, e.g., only at the entry to an environment. These findings align with Hayes et al.’s [291] results discussed above.

Also Biehl et al. [93] investigated privacy concerns of recording technologies (location, video, motion, keyboard activity, schedules, availability, and proximity) in three different environments (office, home, and elsewhere). They found that users were concerned about these technologies and wanted to be informed about the entire process of data collection, processing, and forwarding (e.g., used sensors, access frequency, fusion and aggregation, or storage). However, the role of and relationship with data receivers as well as the purpose of
recordings and its involved utility for users were the strongest influence factors of privacy concerns. But, as concluded by Biehl et al., being aware of how data is collected and processed (e.g., aggregated on group level, accessed only every 15 minutes) could further decrease those concerns.

In the summary of identified influence factors in Table 4.3, we can see that most studies primarily investigated awareness aspects of privacy in video and recording systems. However, several studies found that manual control of such systems is often desired by participants.

4.5 PRIVACY IN SMART HOMES AND AAL

The smart home and related applications of Ambient Assisted Living (AAL) are popular domains in UbiComp research, as discussed in Section 2.3. Factors that have been identified to influence privacy awareness and control in this context are summarized in Table 4.4. We discuss the related user studies in the following.

UbiComp systems in this domain are often based on the detection or recording of users’ activities. Choe et al. [151] conducted a large scale study on what activities and habits people would not want to be recorded at home. The most frequently mentioned activities fall into the categories of self-appearance (e.g., walking in underwear), intimacy (e.g., sex or kissing), cooking & eating, media use, and oral expressions (e.g., singing or phone calls). People were most concerned about recordings taking place in the bedroom, living room, and anywhere in the home, which often involves private conversations, walking in underwear, and intimacy. In a followup study, Choe et al. [152] investigated users’ perceptions and acceptance of sensing and inference systems at home that allow to infer a user’s activity (e.g., vacuuming, sitting, or brushing teeth) based on captured video, audio, electricity use, and movement. They found that video recording was perceived as too intrusive and was only accepted in specific situations (e.g., for a video game system) or for a security system when not being at home. However, participants tend to accept such recording technologies if the perceived benefits outweigh perceived privacy risks. The perceived risk is influenced by what is being captured, how the data is used and who has access to the data. Interestingly users did not want sensing devices to be visibly installed in their homes but instead preferred proper notifications or timely reminders about when devices are sensing.

While notifications about recordings are a reasonable requirement for privacy awareness in smart homes, they also pose the risk of causing undesired disturbances and thus could negatively influence territorial physical. Via field studies in 10 different homes Vastenburg et al. [665, 664] investigated the factors influencing users’ acceptability of notifications at home. They found that the most influencing fac-
tor is the perceived urgency of a notification (e.g., smoke warning or medication reminders), while the timing and users’ activity (e.g., watching TV, cooking, or working) were found to be less important. However, how exactly the urgency of a message is assessed by users depends on several additional context factors, which have not been investigated in Vastenburg et al.’s study. Further influence factors for the acceptance of a notification were found to be the user’s current attention level and a notification’s presentation modality (i.e., whether it is presented intrusive or non-intrusive).

Also Warnock et al. [680] investigated the presentation modality of notifications at home with focus on their effect on error rate and success of users’ current tasks. Their results suggest that the modality does not influence task efficiency, but both wanted and unwanted

Table 4.4: Main factors influencing privacy awareness (◦), privacy control (+), or both (⊕) in smart homes and AAL. Studies reveal insights on privacy-affecting observations (⊿) and disturbances (◂).
notifications reduce error rate and task success. While they did not investigate users’ acceptance of notifications, these results however show that unwanted notifications at home should be minimized.

Little et al. [412] conducted a large scale study with 325 UK citizens in 38 focus groups to examine the privacy concerns of typical UbiComp applications at home. The most prominent factor discussed by participants was who might have access to sensitive information. Furthermore, participants’ relationship to the information receiver crucially influenced their willingness to share. Most were concerned about information leaking outside the family. However, even if information was shared with close family members, participants stated that sharing still depends on what, where, when, and why information is shared. Participants desired systems to be transparent in terms of their data handling practices (e.g., storage, mining, and forwarding to third parties), and to be accessible in terms of providing users with tools for verifying and changing their data if needed. The acceptance of UbiComp applications at home was generally influenced by the convenience and benefits such systems would provide.

Several smart home applications have been proposed to support the live of elderly at home, see Section 2.3. Melenhorst et al. [448] studied elderly’s acceptance and privacy concerns of five smart home systems of the Georgia Tech Aware Home involving video and audio recordings, and location tracking. While most privacy concerns were related to information privacy, one system raised territorial privacy concerns. The FaceBot, a robot with an artificial face was perceived as too physically intrusive and thus could cause undesired disturbances. In general, participants were often concerned about who would have access to their information and who would manage the systems. Melenhorst et al. found that the acceptance of systems was influenced by their relationship and trust in those persons, and by the provided safety benefits of systems. In general people would accept monitoring technologies when they can decide on their own by whom, where, when, and why the monitoring is happening.

Similar results have been reported in the more recent work by Shankar et al. [587] who examined privacy concerns of eight commercial technologies and prototypes for supporting older adults at home. They found that the activity was the most sensitive information type and that concerns about location privacy often stem from the activities connected to a specific location. The perceived benefit mostly influenced the acceptability of systems, for instance safety applications were preferred to socialization applications. All participants were concerned about who has access, what data is collected and at which granularity, where the technology is located, and how the data could be accessed or corrected, which is similar to the results discussed by Little et al. [412]. Furthermore, participants expressed the need for manually pausing the recording of specific systems.
The need for manual control was also expressed in other studies about elder-care monitoring systems [129, 669]. Caine et al. [129] found that participants desire the ability to temporarily switch off individual devices instead of the complete system. Most wanted to switch off video cameras in particular. Interestingly participants were concerned about caregivers having access to the on/off status of devices showing that control decisions should also be considered privacy sensitive and that privacy controls should support plausible deniability strategies. In a field trial of an activity monitoring system conducted by Vines et al. [669], participants were highly concerned about the lack of control. Caregivers could access activities, temperature, and light levels of several rooms in participants’ homes. Participants wished a higher level of control to decide who and when someone could observe them, and desired better feedback on when a device is active.

Providing control and better feedback could increase acceptance and even lower undesired disturbances as demonstrated by Riche et al.’s MarkerClock [534], a display to exchange social and care information between elderly neighbors. The reciprocal nature of the display allowed participants to balance their privacy with their need for care, enabled them to coordinate activities, and to manage interruptions by others. Birnholtz and Jones-Rounds [98] also found that the ability of mediating interactions was an important factor for older adults. Participants desired control mechanisms that allowed them to avoid interactions with others in a similar fashion as it is enabled by attributes of the physical environment. For instance they would prefer having physical places the can go to when they do not want to interact with others. An example for disturbing technologies were cell phones, which frequently caused undesired disturbances in times they wanted to be alone and not be interrupted by others.

Vines et al. [669] found that privacy concerns were further increased by some misconceptions of the monitoring system (e.g., some participants thought that the system is recording video), an issue which has also been identified earlier by Beckwith et al. [80]. This shows that awareness about how information is collected and processed is necessary for users’ privacy risk assessment. Similar to Shankar et al. [587] and Choe et al. [151], Vines et al. [669] found that privacy concerns about the own location often stem from sensitive activities that are connected with a specific location.

Courtney et al. [168] investigated elderly’s privacy concerns of four smart home monitoring systems (bed monitor, motion monitor, kitchen safety, and fall detection). While most concerns raised focused on the video-based system for fall detection and the motion monitor, they found that the perceived benefit of those technologies could outweigh privacy concerns. Their results indicate that the perceived benefit is influenced by users’ self perception of health, physical condition, mental and
emotional condition, anticipatory living, family and friend, healthcare professionals, the physical environment, the technology type, and the perceived redundancy of the technology. The diversity of these factors highlights the strong individual character of perceived benefits for users.

Also the results of a large scale online survey by Beach et al. [79] suggest that acceptance of such care technologies are strongly influenced by the own physical condition and the resulting perceived benefit. This factor is especially important for chronically ill patients and could lead to changing privacy attitudes over time [490]. Beach et al.’s study further confirms that privacy concerns are influenced by the information being shared, with whom it is shared and how it is collected.

Similar findings have been reported by Little and Briggs [411], and Orwat et al. [495]. In addition to what data is collected, with whom it is shared and for what purpose, Little and Briggs [411] found the transparency of how data is stored and mined as further influencing factors for elderly’s privacy concerns. In two case studies of medical care systems, Orwat et al. [495] found that privacy concerns are sometimes neglected when the medical benefit is high enough, e.g., in emergencies. However, even in emergencies people desired transparent regulation about what information is shared and with whom. In general, users wanted to control when and with whom their data is shared.

Hayes and Abowd [290] examined privacy concerns in caregiving monitoring applications for children with learning and healthcare disabilities. While they found that awareness and control over monitoring applications are an essential requirement, the purpose and its associated perceived benefit of such applications fundamentally influence privacy concerns.

The resulting factors influencing privacy concerns in smart homes and in related AAL applications are summarized in Table 4. We can see that dominating factors people want to be aware of in such systems are who has access to a monitoring system or specific information, to what type of information, and for what purpose. Being aware of the purpose in turn enables people to evaluate the benefit provided by the system.

Motivated by the results of existing user studies we conducted an online survey (n=79) and a focus group session (n=9) to further explore the privacy concerns of older adults about smart technology and AAL. We will describe the procedure and results of both studies in the following.
4.6 ONLINE SURVEY: PRIVACY CONCERNS IN AAL

We conducted an online survey in collaboration with the Center for General Scientific Education (ZAWiW) at Ulm University. The survey was advertised through ZAWiW program flyer for the fall academy 2013, which is a one week academic program at Ulm University for seniors interested in current research and scientific education. Parts of the survey results have been described by Schaub [568] but without investigating results pertaining to our concept of territorial privacy. We will focus on these results in the following sections.

4.6.1 Methodology

The survey consisted of seven parts: a) an introduction, b) a scenario-based privacy assessment, c) personality traits, d) technology attitudes, e) social desirability, f) privacy predisposition, and g) information about demographics and health conditions. One goal of the survey was the investigation of privacy preferences in relation to personality traits in order to operationalize general privacy preferences for dynamic privacy adaptation. Detailed materials and results of this investigation are discussed by Schaub [568]. In the following we will limit the discussion of the methodology and results to the parts of the study investigating participants’ preferences and concerns about privacy awareness and control that have not been discussed by Schaub.

As part of the scenario-based privacy assessment, participants were faced with 8 different AAL scenarios (S1-S8) motivated by typical AAL applications which have been discussed in Section 2.3.3:

- **S1 – Health monitoring**: The user in this scenarios suffers an increased health risk caused by cardiac issues. A wrist band equipped with different sensors continuously measures vital parameters (e.g., heart rate, blood pressure, blood oxygen, or sugar levels). The collected health data can be viewed on the own TV and can also be forwarded to third parties (e.g., a doctor, caregivers, or family members).

- **S2 – Emergency notification**: As an extension of S1, the wrist band has the ability to recognize critical health states and can alert third parties about an emergency.

- **S3 – Automatic door opening system (TV)**: The door of the user’s apartment automatically opens to authorized persons. Persons in front of the door are identified and authenticated through a video camera above the door. If a person is not recognized or authorized, the system can ask the user for a manual decision.

---

1 The study was designed in collaboration with Florian Schaub.
In this scenario the user watches TV, and notifications are shown on the TV screen when someone is standing at the door.

- \(S_4\) – Automatic door opening system (bed): Instead of getting notified by the TV, the user receives door notifications by a smart alarm clock while the user is sleeping.

- \(S_5\) – Automatic door opening system (emergency): This scenario is a combination of \(S_4\) with the emergency system described in \(S_2\). Thus, the door announces if someone is at the door and the user can decide to open the door via a voice command.

- \(S_6\) – Smart medication dispenser: The user of this scenario is supported in taking medication daily. The smart dispenser monitors medication intake, can remind the user to take medicine in appropriate intervals, and can forward information about forgotten medications to third parties similar to \(S_1\).

- \(S_7\) – Hazard prevention: In this scenario the user suffers from dementia. The current activity is recognized through ambient sensors in the apartment and devices’ on/off switches. Based on the activity, potentially hazardous situations can be detected (e.g., a stove not turned off) and preventive actions can be triggered accordingly (e.g., automatically switching the stove off). Similar to \(S_1\) and \(S_6\), a detected hazardous situation can be forwarded to third parties in order to inform them about the user’s condition.

- \(S_8\) – Barrier-free phone calls: Ambient speakers and microphones are installed in the user’s apartment in order to enable barrier-free phone conversations. This way phone calls can be seamlessly made anywhere in the apartment without holding a phone. As in \(S_7\) the system is able to detect the user’s activity and can automatically accept calls based on the current activity.

While \(S_1\), \(S_2\) and \(S_7\) are focused only on observation aspects, the other scenarios also involve aspects of disturbances.

For each scenario, participants were asked to rate six statements related to awareness and control on a 5-point Likert scale:

1. In this scenario, I would find it important that I could inform myself about who has access to […]

2. In this scenario, I would find it important that I could control who has access to […]

3. In this scenario, I would find it important that I could inform myself about what information is accessed.

4. In this scenario, I would find it important that I could control what information is accessed.
5. In this scenario, I would find it important that I could inform myself about the purpose of access. (*why*)

6. In this scenario, I would find it important that I could control for what purpose [...] is accessed. (*why*)

Statements 2 and 3 have been omitted in scenarios S3, S4, S5, and S8, as no personal information was involved in these scenarios.

### 4.6.2 Results & discussion

From the 142 persons who participated in the survey, 80 completed it. However, one person did not fit the target group (age=31) and was thus removed from the dataset resulting in 79 samples with a median age of 69.5 years (σ=9.61). The gender distribution of the remaining 79 participants was quite balanced: 46.8% female and 49.4% male (3.8% did not specify gender). Most participants (86.1%) reported to be retired and to have completed an apprenticeship as their highest education level (53.2%). A university degree was owned by 27.8%, and a doctoral degree by (10.1%). All participants were German.

The results of the rated statements are depicted in Figure 4.1 showing a strong desire of the tested awareness and control aspects for all 8 scenarios, which confirm the findings discussed in the previous
sections. While significant differences could be neither identified between scenarios nor between awareness and control, the desire for having the ability to inform oneself about privacy implications was slightly rated higher than the desire to control privacy implications for all scenarios. This highlights that providing awareness about privacy implications is an essential requirement for those and similar UbiComp scenarios and that control mechanisms alone could not satisfy user needs.

The strongest desire was expressed for informing oneself about who has access to information, which conforms to the results reported by several other studies discussed in the previous Section. S3 and S4 show the highest agreement on this aspect, which likely stems from the fact that the door opening system poses high privacy and security risks when the door is opened for the wrong persons.

Interestingly being informed about the purpose of a privacy implication received the strongest agreement on the automatic door opening scenario while watching TV (S3). This might be caused by the fact that the reason for opening the door was not implicitly communicated by the scenario’s description and thus participants tended to prefer receiving more information.

The results support the findings of existing studies discussed in the previous sections and show that all tested influence factors of privacy awareness and control were considered as very important. However, it must be noted that through the nature of an online survey, only seniors with internet access and basic technical skills participated. Furthermore, the results are limited to a German population, which might be influenced by existing social and cultural norms.

4.7 FOCUS GROUP: PRIVACY CONCERNS IN AAL

In order to gain more qualitative insights about older adults’ privacy concerns in AAL, we conducted a focus group session with 9 German seniors with an age ranging from 65 to 76 (M=70, σ=3.84). Five participants held a university degree, one a doctoral degree, and three completed an apprenticeship as their highest education level. The session took place as part of a two hour seminar during the ZAWiW fall academy 2013 at Ulm University.

4.7.1 Methodology

The focus group was held as a semi-structured interview with open discussions following each question. After briefly introducing each other, participants provided demographic information through a short questionnaire and signed a consent form for agreeing to audio recordings. A short (15 minutes) introduction to AAL was followed by the presentation and discussion of three scenarios. Similar to our online
survey, the scenarios were motivated by popular AAL applications already available as commercial products or as prototypes in research projects (see Section 2.3.3). Furthermore, the scenarios involved both forms of potential territorial privacy implications, i.e., observations and disturbances, see Section 3.2.4.

- **S1 – Health monitoring:** The first scenario is similar to S1 used in our online survey. Vital parameters are continuously measured by a sensor wrist band. Health information is forwarded and analyzed by a AAL system at the user’s home. The system can forward the information to third parties (e.g., a doctor, caregivers, or family members).

- **S2 – Positioning:** This scenario extends S1 through a positioning feature. The wrist band is equipped with a GPS sensor to enable localization outside the home. Pressure sensors on the floor of a user’s home enable indoor localization. The current location can be accessed by third parties (e.g., family members or emergency service).

- **S3 – Barrier-free phone calls:** The last scenario is similar to S8 of our online survey with the exception that the speaker and microphone are integrated in the wrist band allowing seamless phone calls even when not at home. To increase the potential invasiveness of the feature with respect to privacy-affecting disturbances, incoming phone calls are suggested to be automatically accepted after three vibration notifications.

After each scenario, the moderator asked probing questions about the perceived usefulness and perceived privacy concerns of the presented system to initiate the discussion between participants. Participants were asked to discuss situations in which they would use the respective system and under what conditions. At the end of the session, participants were asked to provide a sketch on how they view the privacy implications of the wrist band. The goal was to gain insights about participants’ mental models and has been previously applied to study mental models to web security [242], home networking [519], or privacy implications of WiFi networks [359].

### 4.7.2 Results

The audio recordings of the complete focus group session were transcribed, which resulted in 98 individual statements of participants. The data was analyzed using grounded-theory [167]. After an initial open coding phase of the transcript, a code book with 31 data codes was identified and iteratively refined, which resulted in 16 codes and 6 major themes that were used in the analysis:
a) system functionality  
b) mental and physical condition of target group  
c) perceived utility / benefit  
d) privacy implications  
e) social implications  
f) financial implications

The transcript was independently coded by two researchers. The inter-coder reliability was calculated via Cohen’s Kappa and showed an almost perfect agreement ($\kappa = .83$). In the following, the quoted statements of participants have been informally translated from German to English.

**Privacy concerns**

All nine participants agreed that the three scenarios would raise severe privacy concerns and that they would rather not use the technology if not absolutely required. Perceived privacy concerns were primarily influenced by the information’s recipient (who), the system functionality such as automation level and access granularity (how), and the perceived utility and benefit of the system (why).

Most (7) participants stated to accept sharing of health information and even of their own location only with trusted entities (e.g., close family members, care givers, or a doctor), and only under specific circumstances: “I would accept this [...] in a situation in which a doctor told me that my parameters must be monitored for a while – than even continuously and with instant access by the doctor. But after that it must be stopped again” (P3). “Care givers [should have access] only if necessary. But when I think that I can handle things alone, I want to decide [who has access] on my own” (P4). These aspects are also reflected by P4’s sketch of perceived privacy implications, shown in Figure 4.2.

Manual control of access was a strong desire of many participants reflected in several concerns expressed about the system’s functionality: “I could think of a watch that would allow me to trigger an emergency call, but only if I could manually trigger the call” (p2). “Even if I could accept such a system during some periods of health issues, I would not want the system to automatically forward this information. I want to have control over this!” (P4). “This scenario (S2) is unacceptable to me – an active system that automatically forwards information. A passive system with an emergency button would be under some certain conditions useful” (P7). Also P8’s sketch of perceived privacy implications (Figure 4.2) shows the rejection of sensed information being automatically forwarded.

The perceived utility and acceptability of the system was strongly associated with the mental and physical condition of the system’s
target group in which most (8) participants did not see themselves to be included yet, even though they were between 65 to 76 years old: “it would be useful when being older” (P7, age=66); “I think it (S2,S3) is useful and necessary […] I think of my mother […]” (P4, age=65); “I can only think of such a system (S2) for acute fall-prone persons” (P3); “the only situation this (S2) could be accepted is for persons with serious dementia” (P2, P5).

Most participants perceived the need for the technology as well as their own health risks that would warrant it as low. For example, P8 stated ironically that “it’s like we are suffering a heart attack once a week.” Being free from such “surveillance” (P3, P7) did even outweigh the benefit in case of an emergency for three participants: “I cannot think of such an intrusion into my personal freedom. I’d rather think: When I’m on the go and it happens (an emergency), well than it happens. Maybe I’m lucky and someone will find me. – I want to have the freedom to go wherever I want […] without someone in the background, no matter how familiar this person is.” (P3); “I’d consider if I really want to be exposed to such a control or if I’d rather accept the consequences. My God, than it’s just over. – I don’t want to have a watchdog. Sometimes I want to act irrationally” (P7). “For me this would be the opposite of self-determined living” (P2). The perceived invasion on personal freedom by the wrist band is also clearly reflected by the sketch of P7 showing the user in jail (see Figure 4.2).

These opinions underline the high value of self-determination and personal autonomy that could be invaded by AAL systems if they do
not respect individual user concerns and do not integrate appropriate mechanisms for personal privacy awareness and control.

The potential disturbances caused by scenario S3 were also reflected by 6 participants, e.g. P2, P3, and P7: “well I could imagine the voice command function but not an automatic phone call acceptance” (P2). “When I’m in a conversation with someone, then this thing (the wrist band) automatically turns on, this would be the worst of all. It never should turn on automatically” (P7). “I don’t need to be available all the time […] then sometimes I’m just not there” (P3).

Social implications

In addition to the invasion of personal autonomy and privacy, several other social implications have been identified that influence participant’s acceptance of the presented systems. A common concern mentioned by 5 participants was that such systems would cause psychological stress and cognitive dependency:

“When I daily look at my vital parameters I would think about what can be wrong with me. […] I would consider this as psychological strain” (P1). “When everything is recorded and I can see changing parameters, I would worry what’s wrong. But it’s nothing to worry about. That would confuse me and drive me crazy. I don’t want that” (P8). “I don’t want to know that. I don’t want to check my values (health parameters)” (P3). “If the value is out of the norm than I will become sick by myself” (P1). “If I would own such a system I would get [a heart attack]” (P7). “I think one will put oneself in cognitive dependency” (P8). The sketch of P5 does also reflect these concerns, see Figure 4.2.

Another concern was the increased pressure to justify own behavior: “You already see it with the long-term ECG. You are being asked “what have you done at 2pm? Why was your pulse that high?”” (P7). “One risk of such assistance systems is the pressure to justify. When I’m out of the norm […] and suddenly the blood pressure increases they say “what’s now going on?” Then I have to add something in order to allow them to see “ah, he just climbed up this hill” or “now he has drunk two bottles of wine”” (P8).

A decrease in social values was also feared by three participants (P3, P7, P8): “Such systems change (social) behavior. When I can assume everything is managed (by the system) than I might not be able to handle the situation when something broke down. – Than there is no one who will help you in this situation” (P8). “When someone falls over on the street, then it’s his own fault when he is not wearing a wrist band (cynical). – It really is a bit like that, such systems can dissolve social connections” (P7).

4.7.3 Discussion

Our findings confirm previous results from qualitative user studies on AAL, in particular those of Lorenzen-Huber et al. [417] and Courtney et al. [168] (see also Section 4.5). The acceptance of AAL tech-
nology is primarily influenced by the perceived usefulness of such systems depending on the own physical and mental condition. For our participants, the trade-off between health risk and invasion of personal privacy and autonomy mostly leads to a rejection of the technology, with participants accepting negative and even fatal consequences. This might be caused by the good physical and mental conditions of participants and them being in their sixties or seventies (max. 76), which is still younger than the overall population of older adults in Germany. However, it highlights that the technology is not accepted as a preventive mean, but rather as a requirement only for persons with explicit issues of physical or mental health. And even then it is only accepted with clear access restrictions to trusted persons (who). In order to support users in making this trade-off, communicating the purpose of an AAL system and its involved privacy implications (how & why) is essential.

The functionality and especially the automation level of the AAL systems did further influence the acceptance. Automatic forwarding of information and automatic acceptance of phone calls were strongly rejected by our participants. They rather preferred manual control (e.g., in form of a simple button) even in case of an emergency. This highlights that awareness about privacy implications is not sufficient for those technologies and control must be integrated in order to respect individual privacy preferences.

While the generalizability of our results is limited due to the small group size of 9 persons, they are aligned with existing work on AAL (see Section 4.5) and highlight interesting aspects of the involved privacy and health-risk trade-offs made by potential users of AAL technology. Furthermore, the results support the identification of relevant influence factors on privacy awareness and control, which guide the development of our territorial privacy model.

4.8 summary

Our extensive literature review of existing user studies as well as the results of our online survey and focus group study provide insights into the crucial aspects of awareness and control at the user level. Those aspects can be summarized in awareness and control of privacy implications regarding who affects privacy, how it is affected, and why it is affected, see Figure 4.3. The results of the user studies discussed show that especially who and why are of high priority for users. Thus, it is important to support awareness and control of the recipients of observations and of the sources of disturbances (e.g., persons or services). While for persons the social relationship has been found to be most important, trust and credibility influences privacy concerns associated with service providers.
Why privacy is affected should be clearly stated by a purpose for observations and disturbances. This information was found to be essential in order to enable users to assess and measure privacy implications against the perceived benefit and utility of a UbiComp system.

How privacy is affected further involves the aspects of what the affecting observations or disturbances are (e.g., information type or notification content), when they occur (i.e., context), and how they are performed (e.g., how information is recorded or the modality of an interaction). While for both, observations and disturbances, the context (e.g., activity or location) was found to be relevant, several studies have shown that users often prefer manual control of privacy over indirect control by specifying context-based privacy preferences.

The identified factors guided the development of our framework for user-centered privacy awareness and control in UbiComp, which is discussed in the following chapters.
The major goal of our user-centered privacy framework is to provide a holistic solution for awareness and control of privacy implications in UbiComp that respect observations as well as disturbances. To achieve this goal, the framework consists of different user-level and system-level components as depicted in Figure 5.1. As the central part of the framework, we introduce a new model for territorial privacy which allows to capture conventional informational privacy aspects but also the physical aspects of territorial privacy prevalent in UbiComp. The model is based on a privacy graph which respects the previously identified factors of privacy awareness and control. Thus, it allows to model who affects a user’s privacy, how, and why.

The model supports privacy awareness at the user level by mapping an instance of the territorial privacy graph through a privacy management component. The graph-based approach of the model allows the identification of dependencies between observations and disturbances to support users in making informed privacy control decisions. The privacy model and privacy management component are described in Chapter 6 and Chapter 9, respectively.

The instantiation and maintenance of the model is realized by a privacy engine and is based on the discovery of channel policies which provide information about privacy implications and available control options. Channel policies are introduced in Chapter 7. Discovery and enforcement modules realize the discovery of channel policies as well as the enforcement of privacy decisions at the system level. Different
Figure 5.2: Environment types from personal, shared personal, shared, to public environment with decreasing privacy awareness and control capabilities and increasing required trust.

modules have been developed to handle the diversity of privacy implications and system properties depending on the user’s current environment, ranging from personal environments to public environments. The modules and the privacy engine are discussed in Chapter 8.

In the following sections we describe the different types of environments, followed by an introduction of the concepts and terminologies of territories, boundaries, observations, disturbances, and entities as used in this thesis and in particular by the model for territorial privacy. We have previously published parts of this discussion in [1] and [2].

5.1 Environments

By reviewing existing UbiComp applications (see Section 2.3), we identified four environment types for UbiComp systems with different implications on privacy awareness and control: personal, shared personal, shared, and public environments (see Figure 5.2). On the one hand, these environments reflect common user expectations of privacy (see Chapter 4), and, on the other hand, allow the categorization of different UbiComp systems with similar assumptions on trustworthiness, control capabilities, and collaboration:

- The personal environment constitutes the user’s most private sanctuary, e.g., a personal bedroom. System components in personal environments are considered trustworthy and are under the user’s control, e.g., personal devices or smart home components. Therefore, a privacy management component can be instantiated that is able to discover all privacy-relevant infor-
ation in order to provide a user with full privacy awareness. Furthermore, the system is able to take a user’s privacy preferences into account to adapt system behavior accordingly.

- The *shared personal environment* extends the personal environment and is shared with others. For example the living room or kitchen of a family home. The user still has full privacy awareness but control is mediated between privacy interests of different users in the same environment. Thus, in some situations a user may not be able to fully control system behavior as desired due to conflicting preferences of other users.

- A *shared environment* is accessible to a restricted number of users, whereby an individual has only limited control over the environment. However, in most situations a user can still assume to have full privacy awareness. An example is the work office, where a user shares work space with co-workers. Infrastructure services maybe under control of the building management rather than the users.

- The *public environment* is open to anyone but in most cases out of control of individuals. Governments and public service providers exercise control in such environments. Users’ privacy awareness may be partly supported and strongly depends on the collaboration of deployed systems and the pressure of regulatory bodies, such as data protection agencies or the Federal Trade Commission (FTC).

The personal and public environments are similar in definition to those of Daskala and Maghiros [176]. However, distinguishing between two types of shared environments better reflects a user’s desired level of awareness and control over these environments as well as a user’s different privacy expectations [441] compared to one shared environment. Furthermore, the privacy-relevant assumptions of systems in shared personal environments (e.g., a shared apartment) significantly differ from shared environments (e.g., a shared office).

Furthermore, these environments do not have clear-cut borders, they simply serve as categories which subsume many environments with similar configurations on a continuum from personal to public environment. In general, the more public an environment, the harder it is to provide full privacy awareness and to control the privacy of individual users. Therefore, the amount of trust required to be placed in third parties increases. The individual user must trust the environment that privacy is respected. Therefore, privacy mechanisms in shared and public environments need to be designed from a different perspective than those in personal environments. The environment and the perception of the environment play an important role in establishing trust in the privacy awareness of deployed systems.
For example, a public square overlaid with surveillance cameras does not suggest a privacy-friendly environment. Companies, public service providers, and government agencies can actively shape the perception of shared and public environments by supporting privacy awareness and providing feedback to users. With respect to these environments, we developed several discovery and enforcement modules in our framework to address the different properties of UbiComp systems in such environments.

5.2 TERRITORIES AND BOUNDARIES

Based on typical UbiComp applications (see Section 2.3), the identified privacy implications of UbiComp (see Section 3.4) and social theories of privacy as a boundary regulation process (see Section 3.2) we define different territories and their associated boundaries with respect to territorial privacy in UbiComp: personal territory, physical territory, virtual extended territory, and private territory.

- The personal territory ($T_{per}$) relates to the own body and all personal devices that users are typically carrying around or are wearing on their body (e.g., a smartphone, a sensor wrist band, or an AR glass). This territory is similar to Lehikoinen et al.'s [400] notion of personal space, which combines the self, personal devices and the digital self as an extension to Altman’s [45] theory.

- The physical territory ($T_{phy}$) refers to the environments of a user, which are demarcated by physical boundaries like walls or doors. Thus, a physical territory might refer to a house, a room, or a
car, and it includes all physically present persons and systems. The physical territory is always a superset of the personal territory: \( T_{\text{per}} \subseteq T_{\text{phy}} \).

- Through the inter-connectivity of many UbiComp systems the physical territory can be virtually extended beyond physical boundaries. We call this the virtual extended territory (\( T_{\text{ext}} \)), which entails all connected persons and systems that either can observe or disturb a user in her physical territory through the use of communication technologies. It applies \( T_{\text{phy}} \subseteq T_{\text{ext}} \).

- A user’s privacy expectations and preferences are reflected by the private territory (\( T_{\text{prv}} \)), which relates to Altman’s definition of “desired privacy” [45]. It should encompass only persons and systems from which the user accepts specific observations or disturbances. The private territory is a subset of the extended territory, but not necessarily a superset of the physical territory. Thus it applies \( T_{\text{prv}} \subseteq T_{\text{ext}} \) but not necessarily \( T_{\text{prv}} \supseteq T_{\text{phy}} \). This means that a user may have the ability to exclude physically present persons or systems from his private territory. For instance, a user might want to disable a video monitoring systems in the same room.

Traditionally, users were only able to perceive their physical territory. However, with the increasing prevalence of UbiComp systems in our environments, being aware of the virtual extended territory becomes more and more important. Thus, from a user-centered privacy point of view, the goal must be to provide users with full awareness of their virtual extended territory and allow them to enforce their private territory if desired, which should result in \( T_{\text{ext}} = T_{\text{ext}} \). Altman [45] describes this situation as the optimal privacy state when “achieved privacy” is equal to “desired privacy”.

Thus, the main goal of the system-level modules of our privacy framework is to completely discover the virtual extended territory and adapt it in order to map a user’s private territory.

5.3 Observations and Disturbances

In order to address the privacy dimensions defined in our concept of territorial privacy (see Section 3.2.4), our privacy framework must respect different forms of observations and disturbances. Those forms are motivated by the different sensing technologies as well as automation, actuation and interaction levels used in UbiComp applications, see Section 2.2.4. We distinguish between direct and indirect observations and disturbances (see Figure 5.4), which we briefly describe in the following.
• *Direct observations* on the one hand refer to user-centric (see Section 2.2.4) observations stemming from sensors in the user’s personal or physical territory that directly gather data about the user, e.g., a heart rate sensor, a camera, or a microphone in the environment or on a user’s device. On the other hand, direct observations refer to the exchange of personal information that is associated with the user’s identity between different components of a UbiComp system (e.g., forwarding of health statistics from a AAL monitoring system to a care-giving service).

• *Indirect observations* can stem from user-centric and environment-centric sensors (see Section 2.2.4) in the user’s personal or physical territory that gather information that are not directly related to a user. For instance, a smartphone’s acceleration and GPS sensors, or temperature sensors and usage sensors (e.g., digital switches, smart meters) of a smart home system. Even though such sensors do not directly measure person-related data, they pose potential privacy risks if a room or device can be associated with a particular user. For instance, a smartphone’s GPS sensor can provide a user’s location, and digital switches or smart meters can reveal a user’s activity [271, 549, 458]. Even uncritical environmental sensors such as a humidity sensor can be used to infer a user’s presence [282] (see also Section 3.4).

Indirect observations can also stem from sensors that are able to detect personal items and devices of a user through their wireless communication capabilities. For example, a UbiComp system could detect the presence of a user’s smart card via RFID or of another personal device via its Bluetooth, WiFi, or GSM module, which could result in locating the user on different granularity levels. We will refer to those devices as *observable items* (see Figure 5.4).
• **Direct disturbances** refer to disturbances that are directed to the user with the goal of attracting the user’s attention and often require a reaction or the initiation of a subsequent interaction, e.g., a notification or an incoming phone call.

• **Indirect disturbances** are those emerging from automations or interactions in the user’s personal or physical territory but are not directed to the user, e.g., haptic disturbances by an automated wearable blood pressure unit, or noise coming from a cleaning robot or from automatically closing blinds.

In general, observations (regardless whether they are direct or indirect) are only privacy-relevant if they can be associated with the identity of a particular user. While some observations already explicitly contain a user’s identity (e.g., a video or image), others do not (e.g., a location), even though also those observations not explicitly containing the identity could allow the re-identification of a user [427]. However, many UbiComp applications are based on the assumption that users can be reliably identified and the **user–observation association** can be made (see also Section 2.2.4).

A user’s observable items are typically identified via unique identifiers of its communication modules, such as a MAC address, a device UUID or IMEI number. More sophisticated approaches are based on fingerprinting techniques of a device’s communication characteristics [239, 190].

Also the knowledge about **user–observable item associations** is assumed by many UbiComp applications, either by preconfiguring this associations (e.g., as mobile providers know their clients’ IMSI¹), or by detecting this association during runtime (e.g., by users providing their identity in application profiles or even unintentionally by protocols that communicate the user’s identity in public WiFi networks [64]).

The privacy framework’s discovery modules at the system level need to respect these different forms of direct and indirect observations and disturbances. That is those privacy implications of devices in the personal and physical territory must be discovered together with potential connections to the virtual extended territory. With respect to indirect observations, the discovery modules must also be able to learn the user’s associations with observable items.

5.4 **Entities**

With respect to the formerly described notions of territories, observations, and disturbances, we define an **entity** as any device, system, service, application, or person, that potentially affects a user’s privacy through an observation or disturbance. We refer to entities causing observations and disturbances as **observers** and **disturbers**, respectively:

¹ International mobile subscriber identity (IMSI)
Table 5.1: Examples of physical or virtual and active or passive observers.

<table>
<thead>
<tr>
<th></th>
<th>active</th>
<th>passive</th>
</tr>
</thead>
<tbody>
<tr>
<td>physical</td>
<td>(persons, physical sensors)</td>
<td>(systems, services)</td>
</tr>
<tr>
<td></td>
<td>video camera</td>
<td>smart home system</td>
</tr>
<tr>
<td></td>
<td>heart rate sensor</td>
<td>smartphone app</td>
</tr>
<tr>
<td>virtual</td>
<td>(virtual &amp; logical sensors)</td>
<td>(persons, systems, services)</td>
</tr>
<tr>
<td></td>
<td>activity recognition service</td>
<td>activity sharing service</td>
</tr>
</tbody>
</table>

**Definition 2** An observer is an entity that has potential access to a direct or indirect observation in the context of the user’s current activity.

**Definition 3** A disturber is an entity that is able to intervene in the user’s current activity causing a direct or indirect disturbance.

Note that an entity can be both at the same time (e.g., the autonomous device and the person depicted in Figure 5.4). We further distinguish between physical or virtual, and active or passive entities:

- A **physical entity** is any observer or disturber that is part of the user’s physical territory (i.e., inside of physical boundaries).

- A **virtual entity** is any observer or disturber that is connected to a physical entity through some kind of communication technology and thus is part of the virtual extended territory (see Figure 5.3). Virtual entities can be directly connected to a physical entity or indirectly via multiple intermediate virtual entities.

- An **active entity** is either the source of an observation (i.e., an active observer gathers data in the context of a user’s current activity) or the sink of a disturbance (i.e., an active disturber actively intervenes in the user’s physical territory).

- **Passive entities** are connected to active entities via communication technologies. Passive observers do not create any new observations, but rather use or forward existing observations from other active or passive observers. Passive disturbers do not actively conduct disturbances in the user’s physical territory, but cause them through controlling or triggering other passive or active disturbers.

Tables 5.1 and 5.2 show some examples for observers and disturbers that are either physical or virtual and active or passive entities. Note that disturbers cannot simultaneously be both active and virtual. Thus, in contrast to observers, an active disturber always implies that it is also a physical disturber.
5.4.1 Active observers & disturbers

We further categorize active observers and disturbers into *humans*, *ambient devices*, *personal and wearable devices*, *autonomous devices*, *observable item detectors*, and *logical or virtual sensors*, see Figure 5.4. While active disturbers and most active observers are typically located in physical proximity to the user (i.e., inside or near a user’s physical territory), virtual or logical sensors (see Section 2.2.4) provide an exception and can also be located in the virtual extended territory, e.g., a remote activity recognition service that infers a user’s current activity (a new observation) based on observations from ambient sensors such as motion sensors or a video camera.

In the following we briefly describe the different categories of active observers and disturbers, which we also discussed in [2].

- **Humans** in a user’s physical proximity can observe and disturb in different ways (e.g., visually or acoustically). For instance, a person in the same room can observe what the user is doing, observe what the user looks like, or observe what the user is saying. Depending on the proximity a person can also smell the user or even feel the user (e.g., the heartbeat). An undesired disturbance can happen through a person’s noise, speech, or actions that acoustically, visually, or even haptically disturb the user. Persons in physical range of a user are a special form of entities, because a user is not able to control these entities with respect to her privacy needs. Therefore, optimistic approaches for privacy protection need to be considered for those entities, e.g., privacy signaling mechanisms.

- **Ambient devices** are installed or embedded in a user’s physical environment. Those devices are ambient sensors (observers) such as cameras, microphones, thermometers, humidity sensors, infrared sensors, or pressure sensors. Further ambient devices are ambient actuators or output devices (disturbers) such
as automatic blinds, speakers, or displays that could cause visual or acoustic disturbances.

- **Personal and wearable devices** are located in the proximity of the user’s body, e.g., wearable devices in clothes or a smart watch measuring the temperature or heart rate of a user. Even implanted devices or ingestible sensors could be used to measure blood pressure or the blood sugar level (see Section 2.3.3). Those devices in most cases capture direct observations (i.e., person-related data), which often provide sensitive information about a user’s health conditions or activity. The close proximity of those devices to the user also allows haptic disturbances, e.g., vibrations or pressure changes.

Similar to wearable devices, personal devices like notebooks or smartphones are often located in close proximity to the user but do not necessarily have contact with the user’s body. Personal devices can capture direct observations with cameras or microphones similar to ambient sensors. However, personal devices are often equipped with sensors that gather data about the device state, e.g., accelerometers, digital compasses, proximity sensors, or GPS sensors. Those indirect observations can often be associated with the device owner due to the fact that personal devices are often configured with the user’s identity at an initial setup process.

Disturbances from personal devices can occur similarly to those caused by ambient devices, e.g., visual notifications from LEDs or displays, or acoustic disturbances from built-in speakers.

- **Autonomous devices** represent a special class of active observers and disturbers as they do not necessarily adhere to a central component of a UbiComp system. Thus, mechanisms to control autonomous devices in terms of privacy cannot always be provided by centralized solutions. The privacy implications of autonomous devices range widely and are strongly dependent on the device’s capabilities. For example, a vacuum cleaning robot can disturb the user visually and acoustically or even observe the user with on-board sensors, like infrared sensors or a camera. Another example is a coffee machine that starts to notify the user with blinking LEDs or acoustic signals when a decalcification process needs to be performed. Such devices can also gather the location or activity of a user through indirect observations, e.g., via digital switches of the coffee machine.

- The class of **observable item detectors** refers to active observers that can detect the presence or location of a user’s observable items by their wireless communication technologies. For example, a smartphone is typically equipped with several wireless
communication modules for GSM, WiFi and Bluetooth. Newer devices might also have a module for near field communication (NFC). But also other personal items, like music players, watches, or even sport shoes [561] are increasingly equipped with wireless communication modules.

These communication technologies allow the detection or even precise localization of a device due to their wireless nature. For users it is hard to perceive the presence of such observers as they are not limited by physical boundaries. For example, a GSM base station can receive the signal of a mobile device within a range of several kilometers. Mobile network providers are therefore able to determine their clients’ location based on known base station positions. In a similar way, a WiFi access point can detect nearby WiFi devices in a range of about hundred meters. Based on the communication technology and underlying protocols, a device or item can be identified by a unique ID, e.g., the IMSI number of GSM cellphones, or the MAC address of WiFi modules. If such an identifier can be associated with a user’s identity, these indirect observations pose privacy risks.

- Virtual and logical sensors represent the last class of active observers. Those observers are able to infer new observations by analyzing and combining existing observations received from other active observers. For instance, a UbiComp system that infers a user’s activity based on motion, video, and heart rate observations. It is also a common goal of UbiComp middleware to infer higher level context information from lower level sensor data, see Section 2.2.3, thus such middleware components must also be considered in this context. We refer to this class of active observers as critical observers, because inferring new personal information poses one of the highest risks for privacy in UbiComp. This is especially true when personal information is inferred from indirect observations of environment-centric sensors, e.g., inferring a user’s location by analyzing observations from a room’s humidity sensors [282].

5.5 USE CASES

In order to assist the subsequent discussion of our territorial privacy model and to present the applicability of our framework, we introduce three use cases which are motivated by typical UbiComp applications and already existing systems which frame today’s trends towards the UbiComp vision (see Section 2.3 and 2.4). The three use cases (running, working, and coming home) have been selected to provide privacy implications of observations and disturbances at different environment types during a normal day of the user Alice.
5.5.1 Use case 1: running

Every morning Alice goes running. She always wears a sensor wrist band and takes her smartphone with her. On this morning Alice decides to try a new running track. Figure 5.5 illustrates this track in the public environment with different virtual extended territories at three points in time ($t_1$, $t_2$, and $t_3$).

Because Alice had some cardiac issues before, she has installed a health app on her smartphone, which receives several vital parameters (heart rate, temperature, and skin conductance) as direct observations and the smartphone’s acceleration as an indirect observation in order to infer her current health state. Thus, the health app can be seen as a virtual sensor or critical observer in this use case. In case of an irregular health state, Alice is warned through vibrations and an acoustic notification on her smartphone (direct disturbance). When her health state becomes life-threatening, the app automatically forwards the current health state and location of Alice (received from her smartphone’s GPS sensor as an indirect observation) to a remote emergency service who can provide first aid.

Alice further installed a fitness app on her smartphone, which automatically infers her current activity based on observations of her heart rate, the smartphone’s acceleration, and GPS location. The activity, heart rate and location are forwarded and stored by a remote fitness service in order to provide statistics of her fitness activities. For social motivation purposes, her current activity is also shared with friends of Alice through a social network server. For the first part of
Table 5.3: Active and passive entities of the running use case.

<table>
<thead>
<tr>
<th>observers</th>
<th>disturbers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>active</strong></td>
<td><strong>smartphone (speaker, webcam; surveillance camera)</strong></td>
</tr>
<tr>
<td>passive</td>
<td>health app; emergency service; fitness service; social network server; friends; webserver; anybody; surveillance server; police</td>
</tr>
</tbody>
</table>

Table 5.4: Direct and indirect privacy implications of the running use case.

<table>
<thead>
<tr>
<th>observations</th>
<th>disturbances</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>direct</strong></td>
<td></td>
</tr>
<tr>
<td>heart rate; temperature;</td>
<td>health state warning</td>
</tr>
<tr>
<td>skin conductance; video stream</td>
<td></td>
</tr>
<tr>
<td><strong>indirect</strong></td>
<td></td>
</tr>
<tr>
<td>motion; health state; location; activity</td>
<td></td>
</tr>
</tbody>
</table>

her running track the entities of her virtual extended territory do not change (see Figure 5.5).

At time $t_2$, she passes a corner where a public webcam is deployed (i.e., in her physical territory) and her running track is in the camera’s field of view. The direct observation of the camera’s video stream can be accessed by everyone through a public web server. Thus, her virtual extended territory at time $t_2$ is extended by those entities while running in this part of her track. At time $t_3$, Alice enters the field of view of a surveillance camera that was installed for security purposes in front of a parking area. This time, the video stream is stored encrypted on a central surveillance server and can only be accessed by the police in case of emergency or court order.

Table 5.3 and 5.4 summarize all involved entities, as well as potential observations and disturbances of Alice’s virtual extended territory during the complete running use case.

During her running activity, Alice prefers not to be observed, except for security purposes, emergency purposes, and for sharing her activity with friends. Thus, the public webcam and subsequent entities would be excluded from the private territory of Alice that is defined by her preferences. However, as the running activity takes place in the public environment, Alice is not able to control this webcam in order to enforce her privacy preferences. Thus, making her aware of the privacy issue is the only support strategy in this use case, enabling Alice to choose a different running track next time.
Figure 5.6: Entities in the virtual extended territory of the working use case with observations and disturbances. Alice’s private territory cannot be completely enforced because of the settings of the shared environment.

5.5.2 Use case 2: working

Alice works as a research assistant at a university and shares her office with Charlie. Their office (shared environment) is equipped with conventional desk telephones and a remote collaboration system as illustrated in Figure 5.6. The telephones are configured with normal ringtones and allow anybody to initiate a phone call, which would either cause a direct disturbance when calling Alice, or an indirect disturbance when calling Charlie. Charlie can also cause further disturbances, for instance when approaching Alice (direct disturbance) or making phone calls (indirect disturbance).

The remote collaboration system allows to share the availability of persons in an office and to initiate video chats in order to support remote collaboration. The system consists of a wall mounted display with integrated speakers, a camera, and a microphone. A WiFi detector recognizes present persons through RSSI\(^2\) measurements of their smartphones’ WiFi modules (observable item). This indirect observation of available persons is shared with colleagues and students via a collaboration service. To further support awareness about availability, a blurred video stream of the camera is shared between each office and shown on the respective display of the collaboration system. This direct observation enables colleagues (Dave in this use case) to make informed decisions about whether someone is interruptible or not. A video chat can be directly initiated by each colleague. The collaboration system then provides a video and audio stream of the caller, which results in a direct or indirect disturbance similar to phone calls. On an incoming video call, the outgoing video stream remains blurred and the outgoing audio channel switched off until someone in the office

\(^2\) Received Signal Strength Indicator (RSSI)
Table 5.5: Active and passive entities of the working use case.

<table>
<thead>
<tr>
<th>observers</th>
<th>disturbers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>active</strong></td>
<td></td>
</tr>
<tr>
<td>Charlie; WiFi detector;</td>
<td>Charlie; collab. system 1 (display, speaker);</td>
</tr>
<tr>
<td>collab. system 1 (camera, microphone)</td>
<td>telephone Alice</td>
</tr>
<tr>
<td></td>
<td>telephone Charlie</td>
</tr>
<tr>
<td><strong>passive</strong></td>
<td></td>
</tr>
<tr>
<td>collaboration service; students;</td>
<td>collaboration service;</td>
</tr>
<tr>
<td>collab. system 2 (display, speaker);</td>
<td>anybody; colleagues</td>
</tr>
<tr>
<td>colleagues (inc. Dave)</td>
<td></td>
</tr>
</tbody>
</table>

Table 5.6: Direct and indirect privacy implications of the working use case.

<table>
<thead>
<tr>
<th>observations</th>
<th>disturbances</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>direct</strong></td>
<td></td>
</tr>
<tr>
<td>video; audio</td>
<td>incoming phone calls (Alice);</td>
</tr>
<tr>
<td></td>
<td>incoming Video Chats (Alice)</td>
</tr>
<tr>
<td><strong>indirect</strong></td>
<td></td>
</tr>
<tr>
<td>location</td>
<td>incoming phone calls (Charlie);</td>
</tr>
<tr>
<td></td>
<td>incoming Video Chats (Charlie)</td>
</tr>
</tbody>
</table>

accepts the video call. In this case the video stream as a *direct observation* becomes clear and the audio stream as another *direct observation* is switched on.

Table 5.5 and 5.6 summarize all involved entities as well as potential observations and disturbances of Alice’s virtual extended territory in this use case.

Because Alice requires to concentrate on writing an important paper, she prefers not being disturbed and does further not want to share her availability with students. While she is able to control her privacy preferences for her own phone and for the availability sharing, she is neither able to control Charlie’s phone nor able to switch off the shared collaboration system for incoming video calls. Thus, her private territory defined by her preferences cannot be completely enforced, as depicted in Figure 5.6.

5.5.3 Use case 3: coming home

The third use case is located in Alice’s apartment, which she shares with her boyfriend Bob (*shared personal environment*). Their apartment is equipped with several UbiComp systems, which support their daily lives and enhance comfort at home (see Figure 5.7): an *automatic door opener*, an *ambient display*, a *smart coffee machine*, and a *cleaning robot*. With exception of the autonomous cleaning robot, all systems are connected to a central *smart home system*, which coordinates the different
features of their smart apartment. Alice’s observable items are a *smartphone* and a *wrist band*.

When Alice arrives at home, a WiFi detector at the front door recognizes the WiFi module of her smartphone similar to the working use case. This *indirect observation* is forwarded to the smart home system, which identifies Alice and grants her access to the apartment by triggering the automatic door opener. When Alice or Bob are at home the door also automatically opened for friends or family members. The observation of Alice’s presence is forwarded to Bob via a remote *location sharing service* in order to let Bob know that Alice has safely arrived at home.

While the smart coffee machine knows Alice’s and Bob’s bedtimes and automatically makes coffee when they wake up in the morning it still requires manual help by Alice or Bob in order to perform decalcification cycles. Because the next cycle is needed in order to providing coffee on the next morning, the coffee machine reminds Alice with a beep and a notification on the ambient display every 30 minutes. This causes a *direct* acoustic and visual *disturbance*.

In addition, the autonomous cleaning robot is programmed to start a cleaning process before time periods with low electricity rates to save money when recharging. Those time periods are automatically fetched from the Internet. Because the next period begins one hour after Alice has arrived home and a cleaning process does also take one hour, cleaning will start in 5 minutes resulting in a potential acoustic *indirect disturbance*.

Furthermore, the smart home system is able to infer Alice’s activity through a *direct observation* from a video camera and an *indirect observation* from an acceleration sensor in Alice’s wrist band. Based on her current activity the smart home system presents content on the ambi-
Table 5.7: Active and passive entities of the coming home use case.

<table>
<thead>
<tr>
<th>observers</th>
<th>disturbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>door opener; coffee machine</td>
</tr>
<tr>
<td>WiFi detector; camera</td>
<td>cleaning robot; ambient display;</td>
</tr>
<tr>
<td>wrist band;</td>
<td>smartphone (built-in speaker)</td>
</tr>
<tr>
<td>passive</td>
<td>smart home system; location service; Bob</td>
</tr>
<tr>
<td></td>
<td>mobile provider; anybody</td>
</tr>
</tbody>
</table>

Table 5.8: Privacy implications of the coming home use case.

<table>
<thead>
<tr>
<th>observations</th>
<th>disturbances</th>
</tr>
</thead>
<tbody>
<tr>
<td>direct</td>
<td>video</td>
</tr>
<tr>
<td></td>
<td>decalcification notification; latest news; incoming phones calls</td>
</tr>
<tr>
<td>indirect</td>
<td>location; motion; door opener; cleaning robot activity</td>
</tr>
</tbody>
</table>

ent display. For instance, when Alice takes a seat at the kitchen table for having dinner, the display shows her the latest news, which constitutes a direct disturbance. Note, that disturbances can be welcome or annoying depending on the user’s preference and mood.

Alice’s mobile provider delivers incoming phone calls of any person to her smartphone, which can cause direct acoustic disturbances.

Table 5.7 and 5.8 summarize all entities as well as potential observations and disturbances involved in this use case.

Because Alice had a hard day at work she prefers to relax while waiting for Bob and does not want to be disturbed, except for phone calls from friends and family members in case of an emergency (assuming that callers provide the reason for their call as proposed in [265]), and for the door opener for Bob. Thus, her private territory defined by her “do not disturb” privacy preference excludes all undesired disturbers (i.e., the door opener for friends and family members, the coffee machine, the cleaning robot, and the ambient display). Figure 5.7 depicts the private territory of Alice for her privacy preferences in this use case. Because Alice is alone in her shared apartment (i.e., a personal shared environment) her privacy preferences are not in conflict with those of Bob and she is able to control all entities required for enforcing her private territory. Thus, in this situation the environment now provides the same characteristics as a personal environment with respect to provided awareness and control.
5.6 Summary

In this chapter, we provided an overview of our proposed framework for user-centered privacy awareness and control. The main components of the framework constitute a territorial privacy model, several discovery and enforcement modules, and a user-centered privacy management component. We introduced the concepts of environments, territories, boundaries, observations, disturbances, and entities as used throughout this thesis and in particular in the discussion of the territorial privacy model in following chapter. In order to provide a basis for the following discussion of our territorial privacy model and to demonstrate the applicability of our framework, we introduced three use cases (running, working, and coming home), which have been motivated by typical UbiComp applications and existing systems with privacy implications of observations and disturbances in different environments.
Based on the notion of territories, observations, and disturbances described in the previous chapter, we propose a graph-based model for territorial privacy in UbiComp. The model is guided by the conducted literature review and our own results about privacy influencing human factors discussed in Chapter 4. It supports users’ privacy awareness by representing who affects privacy, how, and why, and supports users’ control decisions by identifying appropriate control strategies that enable the mapping of privacy preferences onto available control points. Furthermore, the graph-based approach enables the inference of complex dependencies and interrelations between privacy-affecting actions of entities and to reason about consequences of privacy control decisions.

In the following sections we describe the graph-based model and its main components of entities, channels, and control points, followed by a formalization of the model and a discussion of its applicability for privacy awareness and control. The chapter closes with a discussion of related work. Parts of this chapter have previously been published in [1] and [3]. In [1], we provide a preliminary version of our territorial privacy model, which has been extended in order to respect disturbances as well as graph properties in the following discussion.

6.1 MODEL OVERVIEW

The territorial privacy model is based on the idea of representing all privacy-affecting entities (who) with their potential observations and disturbances (how) as well as the purpose of those privacy implications (why) in a directed property graph. Figure 6.1 shows an example of an instantiated territorial privacy model with a subset of the privacy implications involved in our coming home use case (see Section 5.5.3). In the following, we refer to this example to illustrate the general features of our model, if not otherwise stated.

Privacy-affecting entities are represented as nodes of the graph and their respective observations and disturbances as directed edges, which we call observation channels and disturbance channels, respectively. All entities are connected to a central user node of the graph through one or more observation or disturbance channels. Thus channels represent the flow of observations and disturbances as well as their dependencies. We define channels as follows:

---

1 A property graph is a directed, edge-labeled, attributed multi-graph [539, 540].
Figure 6.1: Example of an instantiated territorial privacy model. The property graph represents privacy-affecting entities $e_1, \ldots, e_6$ as nodes and potential privacy implications as directed edges with observation channels $o_1, \ldots, o_5$ and disturbance channels $d_1$ and $d_2$. Control points represent interfaces for privacy enforcement.

Definition 4 A channel is a direct or indirect connection between an entity and the user that allows this entity to access observations or to cause disturbances of the user’s current activity.

Entities and Channels are further associated with several properties which support modeling how and why a user’s privacy is affected. We briefly describe these properties before discussing different representation levels of the model, followed by a model formalization and a discussion of its applicability.

6.1.1 Graph properties

Entity nodes are associated with the additional properties purpose and location. The purpose property represents why an entity affects privacy by its connected channels. That is, all connected channels of a node are serving the same purpose of this entity. Purposes of entities involved in the example of Figure 6.1 are listed in Table 6.1.

Furthermore, we assume that all outgoing channels of a node depend on all incoming channels of the same node. This allows to model dependencies between different observations and disturbances. For instance, in the example graph, the outgoing video observation channel $o_5$ of the camera $e_5$ depends on the incoming observation channel $o_4$ and both channels serve the purpose of providing a video stream to the smart home system $e_6$. Similarly, the location observation channel $o_3$ depends on $o_2$ and $o_1$. A special case is the dependency of an outgoing disturbance channel on an incoming observation channel, e.g., $d_2$ depends on $o_6$. Such a dependency results in an observation-disturbance cycle with the user node as the start and end point.

Because entities could cause observations and disturbances for different purposes, an entity can be modeled as a logical structure of multiple entity nodes, i.e., one node for each additional purpose.
Table 6.1: Purpose properties of entities involved in the graph of Figure 6.1.

<table>
<thead>
<tr>
<th>entity</th>
<th>node</th>
<th>purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>smartphone</td>
<td>$e_1$</td>
<td>incoming call notification</td>
</tr>
<tr>
<td>location service</td>
<td>$e_2$</td>
<td>sharing location</td>
</tr>
<tr>
<td>friends</td>
<td>$e_3$</td>
<td>$&lt;$unknown$&gt;$</td>
</tr>
<tr>
<td>ambient display</td>
<td>$e_4$</td>
<td>display information</td>
</tr>
<tr>
<td>video camera</td>
<td>$e_5$</td>
<td>providing video stream</td>
</tr>
<tr>
<td>smart home system</td>
<td>$e_6$</td>
<td>providing user activity</td>
</tr>
<tr>
<td></td>
<td>$e_6'$</td>
<td>activity based notification dissemination</td>
</tr>
</tbody>
</table>

Therefore, we define a relation $p^+$ as an additional edge type, which models this logical structure of an entity with multiple purposes. In order to allow the identification of the main entity node with multiple additional purposes, purpose relations are modeled via directed edges. In the example graph, the smart home system $e_6$ has the purpose of recognizing the user’s current activity from the video stream and the purpose of delivering notifications based on the current activity. The latter purpose of the smart home system is modeled in $e_6'$.

The location property represents an entity’s physical, which is required to model physical observers and disturbers inside a user’s physical boundaries. In our example this property would refer to the same physical location for the user node $u$ and entity nodes $e_1$, $e_4$, $e_5$, and $e_6$. The location of the virtual entities $e_2$ and $e_3$ would refer to locations outside the physical boundaries or to an unknown location.

Channels are associated with two additional properties for the channel’s content and state. The content property refers to the content of an observation (e.g., video, activity) or the content of a disturbance (e.g., notification, acoustic noise). In the example graph, the content of each channel is illustrated in red under the respective channel label.

Note that there is a slight semantic difference between observation channels and disturbance channels with respect to the flow of content. In most cases, observation channels represent the way of how personal information is forwarded between entities, e.g., from channel $o_1$ to $o_2$ to $o_3$ in the example. Exceptions are critical observers (see Section 5.4.1), which create new outgoing observation channels from incoming observation channels, e.g., as entity $e_6$. Disturbance channels, on the other hand, represent the way of how entities are able to control or at least trigger physical active disturbers. Thus, disturbance channels between passive disturbers contain events that trigger each other, whereas disturbance channels between active disturbers and the user contain the actual disturbance, e.g., visual display information (disturbance channel $d_1$).

The state property indicates whether a channel is active or inactive. While active channels refer to currently ongoing observations or dis-
turbances in the user’s physical environment, inactive channels refer to potential privacy implications that can become active under certain conditions but currently are not affecting privacy. In Figure 6.1 active channels are colored black, inactive channels gray, representing the situation directly after Alice came home.

Channels as well as entities are further associated with optional control points, which represent available privacy control options for the given user, see Figure 6.2. Control points either allow to control connected channels, a specific purpose of an entity, or the entity itself. In the example graph, control points are given for channel $o_3$ by entity $e_2$, for entities $e_1$ and $e_6$, and for the additional purpose $e_6'$. Controlling channels allows to disable undesired observations and disturbances (e.g., the location observation channel $o_3$ could be disabled if undesired). The control of a purpose allows to disable specific purpose nodes of an entity with all its connected channels. For instance, disabling purpose node $e_6'$ also disables observation channel $o_6$ and disturbance channel $d_2$. Finally, controlling an entity allows to disable the entity with all connected channels and all purpose nodes connected via the additional purpose relation $p^+$. Thus disabling entity $e_6$ would also disable $e_6'$. Modeling control points this way allows the identification of effective control strategies in order to enforce a user’s privacy preferences.

### 6.2 Representation Levels

Entities and channels can be modeled on different representation levels. On the one hand, the applied level depends on the results of the available discovery mechanisms (i.e., it depends also on the current environment type). And, on the other hand, it is influenced by the required detail level for supporting awareness and control. While a higher detail level can provide more awareness and more precise control options, a lower detail level can ease awareness and control by modeling only essential parts of the privacy graph. We will introduce the different representation levels for entities and channels in the following sections.
6.2 Representation Levels

6.2.1 Entity representation levels

While we defined an entity to be any device, software component, or person that can affect a user’s privacy, the entity types are wide ranging and can also have logical or functional hierarchies and dependencies. For instance, the smartphone entity \( e_1 \) in Figure 6.1 could further have functional and logical subentities such as a GPS-sensor, a video camera, or several applications. In order to model such subentities we define the s-relation as an additional edge type in our graph. An s-relation is modeled via a directed edge in order to allow the identification of the parent entity. Thus, a more detailed representation level of modeling parts of the scenario of Figure 6.1 is depicted in Figure 6.3. The location channel is forwarded from the GPS-sensor to the location app and further forwarded to the location service.

In order to support users’ control decisions based on trust and social relationships (see Chapter 4), an entity can also represent a group of persons (e.g., entity \( e_3 \) represents the group friends in Figure 6.1). The same scenario could be modeled with each friend as a single entity node, as shown in Figure 6.3.

On the one hand, modeling entities with logical or functional dependencies could enhance privacy awareness through avoiding unnecessary details. On the other hand, control strategies could be supported by simplifying control or by providing more precise control options when required. For instance, to disable the location channels in Figure 6.3, the GPS-sensor or location app can be controlled. However, if both would not provide any control point, the model allows to identify the smartphone itself as a potential control point to disable the location channel (e.g., by switching it off).

6.2.2 Channel representation levels

Depending on the required detail level for providing privacy awareness and control as well as on the available discovery mechanisms, channel types can be modeled with different semantic levels. Fig-
Figure 6.4: Modeling privacy implications with a high detail level of representation allows to model different channel types. Using virtual channels allows to model a situation at a higher abstraction level.

Table 6.4 shows two different representation levels for parts of the example scenario. If available discovery mechanisms provide a detailed picture of privacy implications, the graph can be modeled at a high level of detail as shown at the bottom part of Figure 6.4. The same graph can be modeled at a lower level of detail if available discovery mechanisms do not provide more information or if more details are not required. We distinguish between the following channel types:

1. A physical channel indicates a direct connection from the user node $u$ to a physical active entity which is able to directly gather data from the user or to physically disturb the user, such as the camera $e_6$ and the ambient display $e_7$ in Figure 6.4.

2. Logical channels refer to observation channels between the user node $u$ and a user’s personal devices or observable items that cause indirect observations, see Section 5.3. For example, the GPS sensor $e'_1$ in Figure 6.4 does not physically observe the user’s location. However, the GPS sensor belongs to the user’s smartphone, which is a personal device associated with the user. Thus, the smartphone’s GPS location corresponds to the user’s current location, which is modeled by the logical channel $o_1$. 
3. **Software channels** represent connections between software components or between hardware and software components, e.g., between the GPS sensor $e_1'$ and the location app $e_2''$ in Figure 6.4. Typically, software channels exist between subentities on the same device, like channels $o_2$ and $o_3$ of the smartphone. A software component itself could again have several subentities connected via software channels. However, whether this level of detail is required depends on the respective use case. Especially important are software channels that contain new derived information based on the content of other observation channels.

4. A **communication channel** represents a low layer connection between two entities with respect to the ISO-OSI reference model [711] (i.e., protocols of the physical and data link layers used by communication technologies such as WiFi, Ethernet, or UMTS). In Figure 6.4 a wireless communication channel exists between the WiFi module $e_1'''$ and the WiFi access point $e_2$. Similar to software channels this channel type allows to model the highest detail level of privacy implications.

5. **Virtual channels** allow to combine one or more underlying channels and entities in order to provide a lower detail representation of the privacy graph. The top graph of Figure 6.4 shows how virtual channels $d_2, o_6$ and $o_8$ can be modeled to provide a high abstraction level of the underlying graph at the bottom. The applied abstraction level depends on the detail level required for privacy awareness and control decision. However, the minimum abstraction level can be determined by adequate discovery mechanisms. For instance, if it is discovered that the virtual channel $o_6$ between the smartphone and the location service is an encrypted SSL connection or the content itself is encrypted, no further detail level is required. If in contrast the channel or content is not encrypted, all underlying entities and channels might affect a user’s privacy as well and thus a higher detail level is desired.

### 6.2.3 Uncertainties

Depending on the environment type as well as technological factors of devices and systems with potential privacy implications, some parts of the privacy graph might involve uncertain aspects. Such uncertainties might result from missing or incomplete discovery processes or discovered channel properties. We model such uncertainties in our graph with channels to an unknown entity $e_u$, see Figure 6.5. A channel to this entity means that one or more other unknown entities might have access to this channel with unknown handling practices.
The reason for this uncertainty is provided by the purpose property of each unknown entity node.

For instance, we assume that the virtual channel \( o_6 \) in the low detail representation level of Figure 6.5 was discovered as an unencrypted channel and the available discovery mechanisms did not allow to gain a more detailed view of underlying entities and channels. We now can model this uncertainty via an additional observation channel from \( e_1 \) to an unknown entity \( e_u \). The purpose property of \( e_u \) in this case will provide information about the unencrypted channel.

Assuming that a detailed picture of underlying privacy implications as in the bottom part of Figure 6.4 could be discovered, and it was further discovered that the communication channel \( o_4 \) is insecure (e.g., unencrypted or encrypted with weak WEP [642]), we can model this insecurity again with a channel to an unknown entity \( e'_u \).

Another example for the need of modeling uncertainties, is a discovered entity that does not provide any information about privacy implications. For instance, it was discovered that the location service \( e_4 \) has access to the location channel \( o_6 \), but the service did not specify how the location is handled further. This uncertainty is also modeled via a channel to an unknown entity \( e''_u \).

### 6.3 Formalization

Formally, our model can be defined as a directed property graph \( G = (V, A, \lambda) \) with the vertex set \( V \), the set of directed and labeled edges \( A \subseteq (V \times T \times V) \), and the function \( \lambda \) as a mapping of vertex and edge properties to respective property values.
The vertex set \( V(G) \) is the union of the user node \( u \) with the set of all entities \( E \) including the unknown entity \( e_u \) and the set of all additional purpose nodes:

\[
V = \{ u \} \cup E
\]

The label set \( T(G) \) (i.e., relation type) is the union of the channel type set including \textit{observation} and \textit{disturbance} \( CT = \{ o, d \} \) with the purpose relation set \( PR = \{ p^+ \} \) for additional purposes and the subentity relation set \( SR = \{ s \} \) for modeling functional or logical dependencies between entities:

\[
T = CT \cup PR \cup SR
\]

Properties of entities and channels are defined as a map from all graph elements \( (V \cup A) \) and property keys \( K = \{ \text{purpose}, \text{location}, \text{content}, \text{state}, \text{controlPoint} \} \) to respective property values \( X \):

\[
\lambda : (V \cup A) \times K \rightarrow X
\]

We define the purpose set \( PS(e) \) of an entity \( e \in E \) as the union of node \( e \) with the set of all additional purpose nodes \( e' \) connected via a purpose relation edge \( p^+ \):

\[
PS(e) := \{ e \} \cup \{ e' \mid (e, p^+, e') \in A \land e, e' \in E \}
\]

All entities \( e \in E \) having the same location as the user node \( u \) or having a location that is within the location of the user node \( u \), are \textit{physical entities}. Therefore, we assume that a user’s location refers to the current physical territory, e.g., a room or defined space. Consequently, we define the set of physical entities \( E_p \) as:

\[
E_p := \{ e \mid e \in E \land \lambda(e, \text{location}) \subseteq \lambda(u, \text{location}) \}
\]

All edges \( (u, c, e) \), with \( e \in E_p \) and \( c \in CT \), are channels between the user node \( u \) and \textit{physical active entities}. Or in other words, an entity \( e \) is a \textit{physical active entity} if it is adjacent to \( u \). Consequently, the \textit{set of physical active entities} \( E_{pa} \) can be defined as:

\[
E_{pa} := \{ e \mid e \in E_p \land (u, c, e) \in A \land c \in CT \}
\]

A path \( P^k = \{(u, c_0, e_0), (e_0, c_1, e_1), \ldots, (e_{k-1}, c_k, e_k)\} \subseteq A \) of \( k \) consecutive entity nodes with \( e_0, \ldots, e_k \in E \) and \( c_0, \ldots, c_k \in CT \) is a set of channels between the user node \( u \) and an entity \( e_k \in E \), denoted as \( \overrightarrow{ue_k} \). Let further \( P^* \) be the set of all existing paths \( P^k \) in \( G \) with \( k \geq 1 \). The set of all \textit{virtual entities} can be defined as:

\[
E_v := \{ e \mid \overrightarrow{ue} \in P^* \land e \notin E_p \}
\]
Further, we define the physical **territory** of a user as the subgraph\(^2\) \(T_{\text{phy}}(V_{\text{phy}}, A_{\text{phy}}) \subseteq G\) containing all physical entities \(E_p\) and the set of their intermediate channels:

\[
V_{\text{phy}} = \{u\} \cup E_p, \quad A_{\text{phy}} = \{u,v \mid e \in E_p\}
\]

Analogously we can define the virtual extended *territory* of a user as the subgraph \(T_{\text{ext}}(V_{\text{ext}}, A_{\text{ext}}) \subseteq G\) by the union of the user node \(u\) with the set of physical entities \(E_p\) and the set of virtual entities \(E_v\) together with the set of their intermediate channels:

\[
V_{\text{ext}} = u \cup E_p \cup E_v, \quad A_{\text{ext}} = \{u,v \mid e \in E_p \cup E_v\}
\]

Let \(E_{\text{per}} \subseteq E_p\) be the set of currently present personal devices and systems in a user’s possession. We then can define the personal *territory* as the subgraph \(T_{\text{per}}(V_{\text{per}}, A_{\text{per}}) \subseteq T_{\text{phy}}\):

\[
V_{\text{per}} = u \cup E_{\text{per}}, \quad A_{\text{per}} = \{u,v \mid e \in E_0 \cup E_v\}
\]

Let \(E_{\text{des}} \subseteq E_p \cup E_v\) be the set of desired entities and \(A_{\text{des}} \subseteq A\) be the set of desired channels as defined by a user’s privacy preferences. We then can define the private *territory* of a user as the subgraph \(T_{\text{prv}}(V_{\text{des}}, A_{\text{des}}) \subseteq T_{\text{ext}}\):

\[
V_{\text{des}} = u \cup E_{\text{des}}, \quad A_{\text{des}} = \{u,v \mid u,v \subseteq A_{\text{des}} \land e \in E_{\text{des}}\}
\]

We further define an observation path \(P^k_o\) and disturbance path \(P^k_d\) as a path with only intermediate observation channels \(o\) and disturbance channels \(d\), respectively:

\[
P^k_o := \{u,v \mid e_0,\ldots,e_k = o \in \text{CT}\}
\]

\[
P^k_d := \{u,v \mid e_0,\ldots,e_k = d \in \text{CT}\}
\]

Let further \(P^k_o\) and \(P^k_d\) be the sets of all existing paths \(P^k_o\) and \(P^k_d\) in \(G\) with \(k \geq 1\).

A cycle \(C^k = \{(u,e_0,e_0),(e_0,e_1,e_1),\ldots,(e_k,e_{k+1},u)\} \subseteq A\) of \(k\) consecutive entity nodes with \(e_0,\ldots,e_k \in E\) and \(e_0,\ldots,e_{k+1} \in \text{CT}\) is a closed path starting and ending at the user node \(u\), donated as \(\overline{u,v}u\). We define an observation-disturbance cycle as:

\[
C^k_{od} := \{u,v \mid e_0 = o \land e_{k+1} = d \land e_0,\ldots,e_{k+1} \in \text{CT}\}
\]

### 6.4 Model Application

The application of the privacy model supports different levels of privacy awareness and control, which is discussed in the following.

\(^2\) Note that it is not an induced subgraph, because a physical entity could also be connected to another physical entity via communication techniques.
6.4.1 Supporting awareness

The graph-based approach supports privacy awareness by modeling *who* affects privacy and *why* in form of entity nodes and their respective purpose properties. The location property does further allow to model whether or not an entity is part of the user’s physical or virtual territory. *How* privacy is affected is modeled by observation and disturbance channels.

One of the primary goals of the graph-based approach is to model dependencies between privacy-affecting observations and disturbances for different purposes and of different entities. Via graph traversals we can infer purpose and channel dependencies to further enhance privacy awareness. Inferring purpose dependencies allows a user to learn for what purpose observation and disturbance channels to physical and virtual entities exist. We define the set of connected *served entities* \( E_{srv}(e) \) to an entity node \( e \) as the union of all subsequent entities connected via outgoing observation channels and incoming disturbance channels. We define the union of those channels as the *served channel set* \( C_{srv}(e) \). Further, we define the union of purposes specified by those entities as the *served purpose set* \( SP_{srv}(e) \) of an entity node \( e \).

Algorithm 1 shows the recursive traversal to subsequently collect served entities and purposes of a given entity via its outgoing observation channels and incoming disturbance channels. Assuming that the entities of the example graph in Figure 6.1 provide the purposes as listed in Table 6.1, the application of this algorithm to entity \( e_1 \) would result in the purpose set (*providing video stream*, *providing user activity*, and *activity based notification dissemination*). Thus, it allows to learn that the camera serves three dependent purposes.

On the other hand, we can leverage graph traversals to learn which entities and what kind of observations and disturbances are required for a specific purpose. For instance, if we know that entity node \( e_6' \), the smart home system, provides the purpose of *activity based notification dissemination* we can infer that this purpose depends on entity nodes \( e_4, e_5, \) and \( e_6 \) with observation channels \( o_4, o_5, o_6 \) and disturbance channels \( d_1 \) and \( d_2 \). We define the resulting *required channel set* \( C_{req}(e) \) of an entity node \( e \) as the union of the required observation channel set \( O_{req}(e) \) with the required disturbance channel set \( D_{req}(e) \), which are defined through Algorithm 2:

\[
C_{req}(e) = O_{req}(e) \cup D_{req}(e)
\]

Further we define the *required entity set* of an entity node \( e \) as the set of all nodes connected to a required channel \( (e, c, e_k) \in C_{req}(e) \):

\[
E_{req}(e) = \{ e | \exists (e, c, e_k) \in C_{req} \}
\]

The algorithm for collecting required channel and entity sets of a given entity node is listed in Algorithm 2. First, it collects all direct
Algorithm 1 Graph traversal to collect sets of served entities, channels, and purposes.

**IN:** graph $G$, entity node $e$

**OUT:** served entity set $E_{srv}$, served channel set $C_{srv}$, served purpose set $SP_{srv}$

**method** `getServedSets(G, e, E_{srv}, C_{srv}, SP_{srv})`

1. add $e$.purpose to $SP_{srv}$
2. mark $e$ as explored
3. for all channels $c$ in $G$.connectedChannels($e$) do
   1. if channel $c$ is unexplored then
      1. if channel $c$ is outgoing observation channel or channel $c$ is incoming disturbance channel then
         1. add $c$ to $C_{srv}$
         2. mark $c$ as explored
         3. $a = G$.adjacentEntity($e$, $c$)
         4. if entity $a$ is unexplored and not user node $u$ then
            1. add $a$ to $E_{srv}$
            2. // recursive call
               `getServedSets(G, a, E_{srv}, C_{srv}, SP_{srv})`
         end if
      end if
   end if
end for

connected channels of the given entity node and recursively traverses incoming observation channels and all disturbance channels in order to find required channels and entities. Disturbance channels are traversed in both directions as a disturbance path must not be interrupted in order to serve a specified purpose. The resulting sets can be used to support control strategies as discussed in the next section.

### 6.4.2 Supporting control

In addition to supporting aspects of privacy awareness, the model supports different control strategies based on the existing control points of entities. The control strategies allow to enforce a user’s *private territory* that is defined by at least one of four different preference sets of entities and channels:

- **desired entity set** $E_{des}$ (permissive rules, default deny)
- **undesired entity set** $E_{udes}$ (restrictive rules, default allow)
- **desired channel set** $C_{des}$ (permissive rules, default deny)
- **undesired channel set** $C_{udes}$ (restrictive rules, default allow)
Algorithm 2 Graph traversal to collect dependent entities with observations and disturbances required for a specific purpose.

**IN:** graph $G$, entity node $e$

**OUT:** observation set $O_{req}$, disturbance set $D_{req}$, entity set $E_{req}$

**method** getRequiredSets($G, e, O_{req}, D_{req}, E_{req}$)

mark $e$ as explored

for all channels $c$ in $G$.adjacentChannels($e$) do

if channel $c$ is unexplored then

if $c$.type is observation then

add $c$ to $O_{req}$

// traverse incoming observation channels

if $G$.sinkEntity($c$) equals $e$ then

$a = G$.adjacentEntity($e, c$)

end if

else if $c$.type is disturbance then

add $c$ to $D_{req}$

// traverse disturbance channels

if $G$.adjacentEntity($c$) equals $e$ then

$a = G$.adjacentEntity($e, c$)

end if

end if

mark $c$ as explored

if entity $a$ is unexplored and not user node $u$ then

add $a$ to $E_{req}$

// recursive call

getRequiredSets($G, a, O_{req}, D_{req}, E_{req}$)

end if

end if

end for

Desired entity and channel sets specify all entity nodes (i.e., entity nodes and additional purpose nodes) and channels which involve privacy implications that are accepted or even desired in a user’s situation. If no explicit undesired sets were specified, a default deny rule is applied for other entities and channels. That is, other entities and channels should be excluded.

On the other hand, undesired sets specify all entities and channels that are not accepted in a current situation and should be excluded from a user’s private territory. In this case a default allow rule is applied, which accepts all other entities and channels in a user’s virtual extended territory when no explicit desired sets were specified.

The different sets are derived from typical aspects of a user’s privacy preferences as discussed in Chapter 4, which include:
1. **Territory based preferences** specify the personal or physical territory as privacy boundaries. Entities outside of these boundaries should be excluded. If the physical territory $T_{phy}$ was specified as the privacy boundary, the desired entity set is equal to the set of physical entities $E_{des} = E_{phy}$. Efficiently enforcing personal or physical boundaries requires the identification of the set of border entities $E_b$ including all entities that are outside of the specified boundary and are connected to a desired entity:

$$E_b = \{ e \mid \exists (e_p, c, e), e_p \in E_{des} \land e \notin E_{des} \}$$

Excluding those border entities will also exclude subsequent virtual entities. In the example of Figure 6.1 this would result in excluding entity $e_2$, the location service.

2. **Entity based preferences** require users to specify the set of desired entities $E_{des}$ or the set of undesired entities $E_{udes}$. The specification of those entities can be made explicitly by listing relevant entities or implicitly based on trust associations with technical entities or social relations to other persons. Observations and disturbances from desired entities are granted while undesired entities should be completely excluded from the private territory.

3. **Channel based preferences** assume that privacy preferences grant or deny specific types of observations or disturbances resulting in the set of desired channels $C_{des}$ or undesired channels $C_{udes}$, respectively. Again these preferences could explicitly refer to specific channels or implicitly refer to a number of channels based on the channel type or content of a channel. While entities are not completely excluded from the private territory, only particular channels are denied.

4. **Purpose based preferences** grant or deny specific purposes for privacy implications. This can either result in complete exclusion of entities or denial of specific channels for the given purpose. Because each purpose is modeled as a separate node in our model, purpose based preferences also result in a set of desired or undesired entity nodes $E_{des}$.

Different preference approaches can also be combined with each other in order to realize more sophisticated privacy wishes of users. The strategy of enforcing a user’s private territory depends on the specified preference sets. We distinguish between three different strategies. The first is applied when only desired sets have been specified, the second strategy when only undesired sets have been specified. The last strategy deals with both desired and undesired sets. All strategies result in decisions on which entity nodes or channels should be disabled via existing control points. After describing the general process of disabling an entity or channel we discuss the different enforcement strategies.
Disabling entities or channels

Disabling a specific entity node or channel depends on available control points, see Section 6.1.1. To disable an entity node \( e \), four different approaches can be applied ordered by efficiency: controlling the purpose, controlling all incoming channels, controlling the entity, and controlling precedent entity nodes of incoming channels, see Figure 6.6.

An available purpose control point allows to disable an entity node with all its connected channels. If this is not possible, the same effect can be achieved when control points for all incoming channels are available. If the entity provides only a central control point (e.g., a device’s on/off switch), it is also possible to disable an undesired entity node via this control point. However, all other entity nodes for additional purposes of this entity (modeled with the \( p^+ \) relation) will be disabled as well. If this is not preferred, control points of precedent entity nodes of incoming channels must be used in order to enforce this privacy preference.

Disabling an undesired channel can be achieved similarly. If no control point is available on either channel side, control points of precedent entity nodes must be used to disable the undesired channel.

Enforcing desired sets

When only permissive privacy preferences in form of desired entity and channel sets have been specified, we can apply an optimistic control strategy which considers all additional entities and channels that are required for the set of desired entities and channels as part of the user’s private territory.

The procedure to enforce this private territory is as follows. For all desired entity nodes \( e \in E_{des} \) and all entity nodes \( e \) that are connected to a desired channel \((e,c) \in C_{des}\), we collect the required entity set \( E_{req}(e) \) and required channel set \( C_{req}(e) \) via Algorithm 2. Let \( E_{req} \) and \( C_{req} \) be the set of all required entities and channels. Now Algorithm 3 checks for all adjacent entity nodes \( e \) of the user node \( u \) (i.e., all physical active entities \( e \in E_{Pa} \)) if their served entity and channel sets contains any required entities or channels \((E_{srv}(e) \cap E_{req} \neq \emptyset)\);
Algorithm 3 Enforcing desired sets.

**IN:** graph G, required entity nodes $E_{req}$, required channels $C_{req}$

**method** enforceDesiredSets(G, $e$, $E_{req}$, $C_{req}$)

for all entity $a$ in G.connectedEntities($e$) do

if entity $a$ is unexplored and not user node $u$ then

mark $a$ as explored

getServedSets(G, $a$, $E_{srv}$, $C_{srv}$, $SP_{srv}$)

if $E_{srv} \cap E_{req} \neq \emptyset$ or $C_{srv} \cap C_{req} \neq \emptyset$ then

enforceDesiredSets(G, $a$, $E_{req}$, $C_{req}$)

else

disableEntity($a$)
end if
end if
end for

$C_{srv}(e) \cap C_{req} \neq \emptyset$). If so, it will recursively proceed with the last step for all adjacent entity nodes. Otherwise, the entity node will be disabled as described before.

Figure 6.7 shows how this control strategy could be applied to our example scenario with $E_{des} = \{e_1\}$ and $C_{des} = \{d_2\}$. The required entity set would be $E_{req} = \{e_4, e_5, e_6, e'_6\}$ and the required channel set $C_{req} = \{o_1, o_4, o_5, o_6, d_1, d_2\}$. The channel control point of $e_2$ can be used to disable non-required parts of the graph.

**Enforcing undesired sets**

If only undesired sets have been specified by a user’s privacy preferences, we can apply a pessimistic strategy which guarantees that all undesired entities and channels are excluded from a user’s private territory. However, also entities and channels that were not specified
Algorithm 4 Enforcing undesired sets.

IN: graph G, undesired entities \( E_{udes} \), undesired channels \( C_{udes} \)
initialize e with u

method enforceUndesiredSets(G, e, \( E_{udes} \), \( C_{udes} \))
  // first remove undesired channels
  for all channel c in G.connectedChannels() do
    if c \( \in \) \( C_{udes} \) then
      disableChannel(c)
    end if
  end for
  // then remove still connected undesired entities
  for all entity a in G.connectedEntities(e) do
    if entity a is unexplored and not user node u then
      mark a as explored
    end if
    if a \( \notin \) \( E_{udes} \) or disableEntity(a) failed then
      enforceUndesiredSets(G, a, \( E_{udes} \), \( C_{udes} \))
    end if
  end if
end for

in the undesired sets might be excluded. The procedure is described in Algorithm 4.

Beginning at the user node u, the algorithm checks if one of the connected channels or one of the adjacent entity nodes (i.e., all physical active entities \( e \in E_{pa} \)) is included in one of the undesired sets. If so, the channel or entity will be disabled as described above. Otherwise, or in case the channel or entity could not be disabled, the same process is repeated with all adjacent entity nodes. This strategy allows to efficiently eliminate larger parts of the graph that involve undesired entities or channels.

Figure 6.8 shows how this control strategy could be applied to our example scenario with \( E_{udes} = \{e_2\} \) and \( C_{udes} = \{o_6\} \). To enforce this preference set the entity control point of \( e_6 \) and the channel control point of \( e_1 \) will be used and exclude undesired parts of the graph.

Enforcing mixed sets

In order to enforce mixed preference sets, we first apply the same strategy as for enforcing desired sets for all desired entities \( e \in E_{des} \) that do not include undesired channels and undesired entity nodes in their required entity set \( E_{req}(e) \) and required channel set: \( \{ e \in E_{des} \mid E_{req}(e) \cap E_{udes} = \emptyset ; C_{req}(e) \cap C_{udes} = \emptyset \} \).

Further we can apply the strategy of enforcing undesired sets for all undesired entity nodes \( e \in E_{udes} \) that do not include desired chan-
After that, only parts of the privacy graph remain that include desired entity nodes or channels with dependencies on an undesired entity or channel. We can now drive a strict or soft strategy. While the strict strategy would exclude all undesired entities and channels resulting in the exclusion of the desired entities/channels, a soft strategy would keep desired ones and accept less privacy by also keeping the undesired entities and channels. Such situations could also trigger explicit user decisions in order to select the best strategy.

Figure 6.9 shows how this control strategy can be applied to the example scenario with $E_{des} = \{e_1\}$, $E_{udes} = \{e_2\}$, $C_{des} = \{d_2\}$ and $C_{udes} = \{o_6\}$. The desired and undesired entity sets are disjoint and not in conflict with each other. Thus, the channel control point of $e_1$ is used again to enforce those privacy preferences. However, the desired channel set depends on channel $o_6$, which is included in the undesired channel set. Therefore, a trade-off strategy is required to solve the conflict in this case.
Supporting manual control decisions

The approaches used in the previously discussed strategies for detecting conflicts between desired and undesired sets, can be leveraged to support manual privacy control decisions of users. For instance, if a user specified the purpose of activity based notification dissemination as a desired purpose and he wants to switch off the camera \( e_5 \), the system could warn the user that this control decision will also disable the desired purpose. Furthermore, if a user wants to manually disable a specific entity that does not provide any control points, the system can propose an alternative control point in order to realize the control decision, based on the strategies described before.

6.4.3 Applying the model to the use cases

In order to demonstrate the applicability of our model to more complex scenarios, we apply it to the three use cases introduced in Section 5.5. For this section we limit the discussion to the coming home use case and refer to Appendix A for details on how the model can be applied to the running and working use case.

Figure 6.10 shows how the graph can be modeled for the coming home use case with entities \( e_1, \ldots, e_{14} \) and their respective disturbance channels \( d_1, \ldots, d_{13} \) and observation channels \( o_1, \ldots, o_{10} \). Table 6.2 shows the allocation of respective purpose and location properties of each entity node. Additional purposes have been modeled for the smartphone \( e_1 \), ambient display \( e_4 \), and smart home system \( e_9 \).
Table 6.2: Properties of entities involved in the coming home use case.

<table>
<thead>
<tr>
<th>entity</th>
<th>node</th>
<th>purpose</th>
<th>location</th>
</tr>
</thead>
<tbody>
<tr>
<td>smartphone</td>
<td>e₁</td>
<td>incoming call notification</td>
<td>Alice’s apartment</td>
</tr>
<tr>
<td></td>
<td>e’₁</td>
<td>&lt;unknown&gt;</td>
<td>–</td>
</tr>
<tr>
<td>wrist band</td>
<td>e₂</td>
<td>provide motion data</td>
<td>Alice’s apartment</td>
</tr>
<tr>
<td>WiFi detector</td>
<td>e₃</td>
<td>provide phone presence data</td>
<td>Alice’s apartment</td>
</tr>
<tr>
<td>ambient display</td>
<td>e₄</td>
<td>display information</td>
<td>Alice’s apartment</td>
</tr>
<tr>
<td></td>
<td>e’₄</td>
<td>display notification</td>
<td>–</td>
</tr>
<tr>
<td>door opener</td>
<td>e₅</td>
<td>automatic door opening</td>
<td>Alice’s apartment</td>
</tr>
<tr>
<td>cleaning robot</td>
<td>e₆</td>
<td>vacuum cleaning</td>
<td>Alice’s apartment</td>
</tr>
<tr>
<td>video camera</td>
<td>e₇</td>
<td>providing video stream</td>
<td>Alice’s apartment</td>
</tr>
<tr>
<td>coffee machine</td>
<td>e₈</td>
<td>maintenance notification</td>
<td>Alice’s apartment</td>
</tr>
<tr>
<td>smart home system</td>
<td>e₉</td>
<td>presence sharing</td>
<td>Alice’s apartment</td>
</tr>
<tr>
<td></td>
<td>e’₉</td>
<td>providing user activity</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>e”₉</td>
<td>activity support</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>e””₉</td>
<td>notification dissemination</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>e”””₉</td>
<td>door access control</td>
<td>–</td>
</tr>
<tr>
<td>location service</td>
<td>e₁₀</td>
<td>sharing location</td>
<td>Stuttgart, Germany</td>
</tr>
<tr>
<td>Bob</td>
<td>e₁₁</td>
<td>&lt;unknown&gt;</td>
<td>&lt;unknown&gt;</td>
</tr>
<tr>
<td>mobile provider</td>
<td>e₁₂</td>
<td>forwarding phone calls</td>
<td>Munich, Germany</td>
</tr>
<tr>
<td>anybody</td>
<td>e₁₃</td>
<td>&lt;unknown&gt;</td>
<td>&lt;unknown&gt;</td>
</tr>
<tr>
<td>friends / family</td>
<td>e₁₄</td>
<td>&lt;unknown&gt;</td>
<td>&lt;unknown&gt;</td>
</tr>
</tbody>
</table>

The smart home system serves five purposes. The first purpose (modeled in e₉) is sharing Alice’s location (observation channel o₄). The second purpose is the recognition of Alice’s activity (observation channel o₄) via the camera’s video stream (observation channel o₆) and motion data from Alice’s wrist band (observation channel o₇), which is modeled in e’₉. Purpose three is modeled in e”₉ and represents supporting Alice’s activity with information shown on the ambient display (disturbance channel d₄). The third purpose is the forwarding of the coffee machine’s notification (disturbance channel d₇), which is modeled in e””₉. The final purpose of e”””₉ is controlling the door opener when friends or family members arrive resulting in the physical disturbance channel d₁.

The smartphone serves the purpose of notifying about incoming calls with disturbance channel d₈ and forwarding the location to the WiFi detector e₃ via observation channel o₂. The smartphone is an observable item of Alice, which is modeled by the location observation channel o₁. While in practice the WiFi detector recognizes the smartphone’s presence, modeling it this way allows us to apply the same awareness and control strategies for indirect observations as for direct observations, e.g., the video observation channel o₈ of the camera.
Alice is provided with control points for entities, purposes, and channels, which allow her to control most physical entities. However, she is not able to control the WiFi detector $e_3$, which is assumed to be an integrated hardware component that cannot be switched off.

Assuming that Alice has the privacy preference as described in Section 5.5 (no disturbances, except for phone calls from friends and family members and except for the door opener when Bob arrives), the undesired entity set $E_{udes}$ is $\{e_4, e_4', e_6, e_8, e_9'', e_9'''', e_{13}, e_{14}\}$, the desired entity set $E_{des}$ is $\{e_{11}, e_{14}\}$ and the required entity set $E_{req}$ is $\{e_5, e_1, e_{12}\}$. Applying the control strategies as described in Section 6.4.2 will result in disabling $e_4, e_6$ and $e_8$ via the entity control points, and disabling $e_1'$ via its purpose control point. Reasoning about the changed conditions and privacy preferences will also result in a new disturbance channel from $e_{14}$ to a new entity node $e_1''$, which represents the allowed phone calls from friends and family members. Another disturbance channel will occur from Bob $e_{11}$ to the door opener via another entity node for the smart home system $e_9$, which represents the other exception of Alice’s privacy preference.

### 6.5 RELATED WORK

Rodden [537] developed a graph-based model of awareness for shared applications in computer supported cooperative work. While he uses a similar approach in order to model spatial relations via a directed graph, the focus is on modeling relations between any kind of object which users may pay attention to or interact with in a shared space. He argues, that the concepts of the underlying spatial model of interaction [87] can also be applied to a virtual space.

Metaxas and Markopoulos [450] extend Rodden’s work to model privacy implications. They align the concepts of focus and nimbus from the spatial model of interaction [87] to the concepts for dynamic privacy regulation of solitude, confidentiality, and autonomy proposed by Boyle and Greenberg [109] (see also Section 3.2.3). The concept of focus is mapped to solitude and is semantically similar to our concept of disturbances. The nimbus can be represented by confidentiality and autonomy, which is similar to our notion of observations. However, the model of Metaxas and Markopoulos only supports inter-person related disturbances and observations in awareness systems (e.g., to model how much attention is payed to another user’s actions or how much information is shared with users). Further, their model neither supports privacy control nor the representation of purpose and dependencies between different observations and disturbances.

Ortmann et al. [493] use a graph-based approach to model information flow in pervasive systems. The graph allows to represent directly and indirectly gathered information. Analyzing the graph further supports the identification of information sources (e.g., sensors),
which need to be controlled in order to avoid undesired information
collection. While their approach is similar to our model applications,
it does not support disturbances and the consideration of purpose.

Jafari et al. [321] propose a semantic model for purpose based on
representing privacy-affecting actions in an action graph. They pro-
vide a modal logic and model checking algorithm for the formal ex-
pression and verification of purpose-based privacy policies. Tschantz
et al. [655] model dependent privacy-affecting actions for a specific
purpose based on a modified version of Markov Decision Processes
(MDPs) for planning. Their approach allows to infer when a sequence
of different actions is for a specific purpose in order to support auto-
matic auditing. While these approaches are similar to the inference of
dependent purposes in our model application, they neither involve
privacy control strategies nor the modeling of disturbance.

6.6 SUMMARY

In this chapter, we proposed a graph-based model for territorial pri-
vacy in UbiComp. The model represents all privacy-affecting enti-
ties (who) with their potential observations and disturbances (how) as
well as the purpose of those privacy implications (why) in a directed
property graph. Privacy-affecting entities are represented as nodes
of the graph. Their respective observation and disturbance channels
are modeled as directed edges which are connected to a central user
node and represent the flow of observations and disturbances as well
as their dependencies. Entities and channels can be modeled on dif-
ferent levels of representation, which allows to cope with different
results of discovery mechanisms as well as different requirements for
privacy awareness and control at the user level. In order to support
privacy awareness at the user level, the graph-based approach en-
ables the identification of complex dependencies and interrelations
between privacy-affecting actions of entities with associated condi-
tions and purposes. Control decisions at the user level are supported
by the identification of appropriate control strategies that enable the
mapping of privacy preferences onto available control points, and
by reasoning about consequences of privacy control decisions. We
demonstrated the applicability of our model by applying it to the
three use cases, which have been introduced in last chapter. The in-
stantiation of the model is supported by the discovery of channel
policies, which is introduced in the following chapter.
The instantiation of the privacy model introduced in the last chapter is based on a discovery mechanism of channel policies. Channel policies specify how and why an entity is affecting a user’s privacy with respective observations and disturbances. In this chapter we first give a description of the general discovery approach of channel policies. After providing an overview of existing privacy policies we describe the structure of our proposed channel policies in detail.

7.1 DISCOVERY PROCESS

The primary goal of the discovery process is the collection of channel policies in order to instantiate the complete privacy graph with relevant entities and their involved privacy implications in a user’s virtual extended territory. The general discovery process is based on an optimistic approach. Therefore, a basic requirement for the completeness of the discovery process is the collaboration of entities. Privacy implications of entities that do not provide channel policies or implications of malicious entities can only be discovered to some extent with pessimistic approaches. We discuss some possible pessimistic strategies in Chapter 8.

The discovery process further depends on the two assumptions that channel policies are associated with a unique identifiable entity and that channel policies provide references to further policies of connected entities. We further assume that the discovery of channel policies and enforcement of privacy preferences is managed by a privacy agent on a user’s trusted personal device. For the rest of this thesis we assume this device to be a user’s smartphone.

![Figure 7.1: The instantiation of the territorial privacy model is based on different strategies for discovering channel policies of privacy-affecting entities in a user’s virtual extended territory.](image)
Discovering channel policies can be realized by combining different strategies (illustrated in Figure 7.1) that are influenced by features of the user’s current environment (see Section 5.1):

- **Personal device discovery** aims at collecting channel policies of entities in a user’s *personal territory*. For instance, channel policies of smartphone applications or personal fitness devices.

- **Infrastructure-based discovery** leverages existing network infrastructures of systems in the user’s *physical territory*. For example, existing home networks and available discovery protocols such as UPnP can be used to collect channel policies of entities. This approach is most appropriate for *personal and shared personal environments* assuming that users have access to and control over the infrastructure. Discovered channel policies allow to frame the *physical territory* and parts of the *virtual extended territory* that belong to the infrastructure.

- **Environmental discovery** refers to strategies for policy collection in environments in which users have no access to the existing infrastructure. Possible mechanisms to allow this kind of discovery are based on wireless broadcasts, visual markers, or a central location-based policy database. These strategies are mostly required for discovering the *physical territory* in *shared and public environments*, e.g., existing surveillance cameras.

- **Virtual remote discovery** collects policies of virtual entities by following policy references in channel policies discovered by one of the previous discovery strategies. Thus, virtual remote discovery aims at framing the *virtual extended territory* and is required as a supplementing strategy in all environments.

Depending on the applied strategy, a single channel policy or a set of channel policies might be received. For instance, personal device and infrastructure-based discovery strategies might provide a central component that holds all relevant channel policies (e.g., a policy manager of a smartphone’s operating system or a policy manager of a smart home system). Thus, the need for virtual remote discovery depends on the completeness of the policy sets provided by other discovery strategies. This completeness could be supported by entities through prefetching subsequent channel policies, thus performing a virtual remote discovery on their own. Such a strategy might be useful for scenarios with static configurations or low dynamics in privacy relevant observations and disturbances, e.g., a public web cam that provides a live video stream on a public website. Here, an environmental discovery approach providing the complete set of involved channel policies would decrease the discovery overhead.

We further distinguish the discovery process between *authenticated discovery* and *anonymous discovery*. Authenticated discovery refers to
the discovery of personal privacy implications that are associated with a particular user, for example the privacy implications of the health app and fitness app in the running use case, see Section 5.5.1. In order to discover such privacy implications the user must authenticate with the involved entities to ensure that the current personalized privacy state of the user is reflected in returned channel policies. In other situations, an anonymous discovery approach might be sufficient. For example, when privacy implications do not differ between users as for the observations from surveillance cameras in the running use case or the disturbances from the cleaning robot in the coming home use case, see Section 5.5.3.

Once the privacy model is instantiated it must be kept up to date in order to always present a user’s current privacy state. The initial discovery process as well as required discovery updates are triggered by several factors:

- *changes in the personal territory* can occur by switching on/off personal devices or starting/terminating applications on a personal device.
- *changes in the physical territory* can be caused by switching on/off devices and systems in the environment, or by moving to other locations.
- *changes in the virtual extended territory* which can arise when virtual entities adapt their privacy practices.
- *context changes* are particular important to determine channel state changes. While some channels might be inactive during times of discovery, they can become active due to contextual changes, e.g., at a specific time or in case of an emergency as in the running use case.

After discussing related policy languages, we describe the structure of our proposed channel policies in detail. The different technical solutions for realizing the discovery of channel policies on the system level will be discussed in Chapter 8.

7.2 RELATED POLICY LANGUAGES

In general policy languages aim to support resource management and control by specifying access rules and constraints in form of policies. Several policy languages exists that allow to formulate such rules for security or privacy management of personal information as the central resource. From a user-centric privacy point of view one can distinguish between *user-defined policies* (i.e., policies that specify a user’s privacy preferences) and *entity-defined policies* (i.e., policies that specify data handling practices and privacy-affecting actions of entities). Channel policies belong to the latter category.
In the following we will discuss policy languages with focus on security and privacy management which propose similar concepts as used in our channel policies. For a more extensive discussion of privacy policy languages we refer to existing surveys [284, 374, 200].

One of the most popular policy languages is the W3C’s Platform for Privacy Preferences (P3P) [169]. P3P provides a standardized and machine readable way for websites to state their data handling practices in form of XML-based privacy policies. The P3P language supports the specification of recipients, data categories, purpose, and retention in one or more privacy statements. Policies can be discovered by different forms of policy references included in HTTP headers, a link tag, or at predefined well-known locations. We adapt the statement and references approach for our channel purposes. While P3P is motivated by typical information privacy issues online, it does not support the specification of privacy-affecting disturbances. Furthermore, P3P focuses on the specification of a website’s local data handling practices. Limited support for discovering data handling practices of third parties to which personal information might be forwarded is provided. Policy references of external entities can be integrated in hint elements.

While P3P supports the specification of a wide range of information privacy aspects, the complexity of the language has led to rare adoption and often to an incorrect use of the vocabulary [403, 170, 422]. Langheinrich [389] adopted P3P for privacy policy specification in his PawS architecture, see Section 3.5.3. He extended P3P’s data scheme with perception and location in order to also enable the specification of privacy implications stemming from the access to sensory data (i.e., camera, microphones, and others sensors) as well as the access to location information.

The Enterprise Privacy Authorization Language (EPAL) [55] has been proposed to complement P3P for enforcing privacy practices in enterprise environments. EPAL policies allow the specification of access rules that define who can perform what actions (e.g., read, write, disclose) on which data categories for what purposes. Purposes are organized in a purpose hierarchy in order to improve the expressiveness of rules and to allow compact policies. They further propose to integrate the concepts of obligations and conditions in policy rules. Obligations allow to define required actions that must be performed when data is accessed, e.g., “erase after 5 days”, or “stored encrypted.” Conditions can be used to bind policies to specific Boolean rules that must be fulfilled for granting access. Such conditions allow to incorporate context factors in access control decisions.

Conditions and obligations are also part of the eXtensible Access Control Markup Language (XACML) [535], which is a similar but more expressive policy language for access control specification compared to EPAL [48].
Related to these policy languages are some access control models with similar objectives. Byun et al. [124] propose purpose based access control as an extension to the conventional role-based access control (RBAC) [226], in which permissions are assigned to functional roles to control the access of subjects to objects. Similar to EPAL, they propose to model the purpose of access control rules in form of a purpose hierarchy. They further distinguish between intended purpose (i.e., the purpose for which data can be accessed) and the access purpose (i.e., the purpose for an actual access). Also Ni et al. [478] extend RBAC with purpose binding, conditions and obligations in their framework for privacy-aware role-based access control (P-RBAC).

Combining contextual conditions with RBAC is also referred to as context-aware RBAC [472, 371]. Neumann and Strembeck [472] extended the design and implementation of an existing RBAC service to allow the dynamic enforcement of context constraints. Kulkarni and Tripathi [371] propose a context-aware RBAC model to deal with the context-based dynamics in UbiComp applications. They integrate their model in a programming framework in order to enable context-based role permissions, context-based permission activation constraints, and context-based resource access constraints. The framework assumes the availability of a context management layer, similar to typical context middleware approaches discussed in Section 2.2.3.

Park and Sandhu [504] aim at covering traditional access control models (e.g., mandatory, discretionary, and role-based) in their more generic usage control model UCON_ABC. The model integrates authorizations (A), obligations (B), and conditions (C). They define obligations as “functional predicates that verify mandatory requirements a subject has to perform before or during a usage exercise.” Thus, they distinguish between pre-obligations and ongoing-obligations. Conditions are defined as “environmental or system-oriented decision factors” which are independent from subjects and objects.

Babbitt et al. [63] built upon the concepts of EPAL to support the specification of access control policies for physical privacy. They introduce the notion of environment objects, which refers to all objects in a user’s environment that can be physically actuated or operated, e.g., automatic blinds or ambient speakers and displays. Thus, this approach allows to explicitly specify disturbance related access control constraints as part of privacy policies.

Toninelli et al. [650] propose a policy model for usable security on smartphones. The policy model supports access control to personal information and to a user’s attention in order to prevent undesired interruptions. Policies are represented as a set of RDF statements or Sparql triples to ease policy reasoning and allow to specify the requester, resource (information or attention), action, and context (e.g., time, location or activity).
While there are several existing privacy policy languages, most of them focus on information privacy and do not respect physical privacy aspects as required by our concept of territorial privacy. Furthermore, several languages are limited to the specification of access control policies and do not allow the representation of privacy implications. Also the specification of dependencies in order to model the information flow of observations and disturbances is not supported by any language. However, some of the discussed concepts are also relevant for the discovery of territorial privacy implications and therefore have been respected in the design process of our channel policy format that we discuss in the next section.

7.3 CHANNEL POLICIES

We propose channel policies as a container format in which entities can specify active and potentially active privacy implications as well as available control points. The general structure of a channel policy is depicted in Figure 7.2. In order to support the instantiation of the territorial privacy model, channel policies provide information in three parts. In the entity description part, channel policies provide entity-specific information. Information about an entity’s observation and disturbance channels is provided in form of one or more channel specifications. Similar to P3P’s privacy statements [169], purposes are specified as one or more purpose statements. Each purpose statement corresponds to one entity node of the privacy graph as described in Section 6.1. We discuss the different parts of a channel policy in the following sections. While channel policies have been realized in XML (see Appendix B for an example of a policy), we apply an abstract illustration and specification of the policy parts in the following description, in order to focus on the underlying concepts.
7.3.1 Entity description

This part of a channel policy provides meta information about the entity that issues the policy. This meta information consists of mandatory parts for identity and type of an entity, and optional parts for an entity’s location, hierarchy, and available control points.

IDENTITY The mandatory identity part provides the major information to determine who is affecting a user’s privacy. The identity is composed of a unique identifier for this entity, a descriptive name, and optional information about the authority and manufacturer of this entity. The identifier should at least be unique in the context of the user’s current environment, e.g., a device’s IP or MAC address. However, an independent identifier such as a UUID\(^\text{1}\) is preferable. A descriptive name should provide a user-friendly description of an entity, e.g., “Nexus 5 smartphone”, “kitchen camera”, “heart rate sensor”, “sports tracking service”, or “facebook friends”.

The authority of an entity does either refer to the owner of an entity or to other regulative or administrative authorities of an entity (e.g., the user herself in case of personal devices or systems, or government agencies and companies in case of public systems). The entity’s manufacturer name can be provided for entities that are hardware and software components.

TYPE The type of an entity describes whether it is a hardware, software, social, or logical entity. The type can be hierarchically composed in order to provide a more detailed description, e.g., hardware.sensor.GPS-sensor or software.application.messaging. Social entities refer

---

\(^{1}\) Universally Unique Identifier (UUID)
to groups (social.group), individual persons (social.individual), or roles (e.g., social.role.medic).

Logical entities can be composed of several other entities with different types. For instance, the smart home system of the coming home use case (see Section 5.5.3) is a logical entity which is composed of different hardware and software components.

**LOCATION**  An entity’s location provides an absolute or relative location cue, which can be composed hierarchically in order to provide more detailed location information. The information is required to determine entities in a user’s physical territory and also provides information about the dimensions of the virtual extended territory. A detailed location cue with absolute and relative location information on different detail levels could look like the following example:

```
country:Germany | city:Ulm | street:James-Franck-Ring |
building:Ulm-University | building-part:o27 |
level:3 | room:3305 | relative:above-door |
coordinates:48.422648,9.957294,636.52
```

The required location granularity depends on the entity type and its physical proximity to the user. A higher granularity would be preferable for physical active entities whereas a coarse location might be sufficient for virtual entities. For instance, a user might want to know the exact location of a video camera in the environment, but might be satisfied with a coarse location (e.g., the city) of a remote service that has access to the video stream of the camera.

**HIERARCHY**  The hierarchy of an entity describes the functional and logical structure of an entity to support the model’s different representation levels as discussed in Section 6.2. Therefore, an entity’s policy can specify a parent entity and one or more child entities. Each entity is referenced via the entity’s type followed by its corresponding unique identifier. For instance, a smartphone entity could specify child entities for an application and a GPS sensor:

```
software.app.4b10a258-9393-4261-b1cf
hardware.sensor.GPS-sensor.277fc65d-949a-4aa5-8870
```

The policy of a group entity could specify the respective group members where the identifier is replaced with the full name of each individual, for instance:

```
social.individual.John-Doe
social.individual.Alice-Allison
social.individual.Bob-Blair
```

**CONTROL POINTS**  Optional control points provided in the entity description of a channel policy refer to available and authorized control options for the user which allow to control entity-specific functions or settings with associated privacy implications. The primary
function of an entity to be controlled via such control points is its
general state of operation, i.e., whether it is on or off. More sophisti-
cated control options could allow to modify schedules or constraints
for operation.

We distinguish between control point references and control point inter-
faces. While control point references point to available user interfaces
of an entity that allow a user to manually control respective settings,
a control point interface allows the automatic control of settings by
privacy enforcement mechanisms.

An example is given in Figure 7.4. The channel policy on the left
specifies only a control point reference of type HTTP-HTML that points
to a URL. Thus, the entity can be controlled only manually by the
user via a web frontend. Another possible control point could specify
a HTTP REST API. The channel policy on the right specifies a control
point reference together with a control point interface. The reference
type Android-local-intent refers to an Android Activity [259] on
the user’s personal smartphone\footnote{Note that we assume an Android smartphone as the user’s central personal device
that hosts a privacy agent. Therefore, we provide examples for Android’s application
framework. However, similar solutions can be found for other mobile platforms.} that allows manual control of an ap-
plication’s settings. The same settings can be automatically controlled
via the interface specification.

The interface specification must provide the list of controllable func-
tions or settings together with allowed parameters. If the control of an
entity should be limited only to authorized users, the interface speci-
fication must further provide an authentication token for the specific
user. This token should be updated with every channel policy and
should only be valid for a short time period (e.g., one day). Including
authentication tokens in channel policies requires an authenticated
discovery process (see Section 7.1) and a secure communication chan-
nel to prevent misuse of the token.

The concrete specification of a control point interface depends on
the entity type. For local applications on the user’s smartphone we
assume that interfaces are specified as intents [260] that allow the

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{example.png}
\caption{Example of different control point specifications in the entity
description of two channel policies.}
\end{figure}
privacy agent to directly control an application, e.g., to terminate or pause an application.

For environmental entities that are part of a user-accessible infrastructure (e.g., in personal or shared personal environments) the interface specification might leverage available control protocols. For instance, in a user’s home network, control interfaces of entities can be specified via existing UPnP [660] control points.

In order to also support the automated control of virtual entities we assume that those entities provide interface specifications in form of a RESTful3 control API.

7.3.2 Channel specification

For each observation and disturbance channel that is connected to an entity, the policy should provide a channel specification, see Figure 7.5. This policy part is composed of an unique channel identifier, the channel type, the channel’s source or sink entity, the current state together with an optional activation frequency, optional information about the protection of the channel in terms of applied security mechanisms, information about the channel’s content, and finally available control points of the channel.

**Identifier and type** A channel’s identifier should be a UUID, which uniquely references the respective channel. For an authenticated discovery process the identifier might refer to a channel that is associated with an individual user. In other cases the identifier for a channel might be the same for all users (e.g., an observation channel of a video camera). Note, that a channel can be specified as an outgoing channel in a channel policy of entity a and as an incoming channel in a channel policy of entity b. Therefore, it is required that the identifier is the same in both channel policies. While one entity might not be able to specify all details of a channel (such as state, protection, or content), the details can be combined by both entities during the discovery process.

The type of a channel indicates whether it is an observation or disturbance channel. The details about the observation or disturbance are provided in the content part.

**Source and sink entity** For incoming channels the identifier of the source-entity is provided, for outgoing channels the identifier of the sink-entity. In order to support virtual remote discovery (see Section 7.1) a policy reference to the source’s or sink’s channel policy should be given for each channel specification. We distinguish between direct policy references and policy base references.

---

3 That is, adhering to the architectural constraints of representational state transfer (REST).
A *direct policy reference* directly points to the corresponding channel policy that needs to be fetched by the discovery process. Depending on the applied discovery strategy, a direct policy reference can be a URL referencing a policy file which can be fetched via HTTP (e.g., `http://uulm.de/smart-home-lab/policy152.xml`). Or it can be a URI referencing a local policy resource on the user’s smartphone, which can be fetched through the application framework (e.g., `android.resource://com.4yourFitness.app/raw/policy`). The drawback of direct references is that the exact location of a policy must be known by the referencing entities in advance. However, direct references can be especially useful for anonymous discovery without personalized channel policies or for entities with fewer variances in privacy implications.

On the other hand, a *policy base reference* points to a location where an entity’s channel policy can be requested by providing the respective channel ID. The entity is then required to dynamically deliver the channel policy associated with the given channel. Following the previous examples, a base reference could be the URL `http://uulm.de/smart-home-lab/policies/` where a channel ID can be concatenated to form a RESTful policy request. For local applications on a user’s smartphone the base reference can be an intent similar to the specification of an entity’s control point interfaces. This allows to provide the channel ID to the local entity which in turn delivers the policy.

**State and Frequency** A channel’s *state* indicates whether the channel is currently active or inactive. An active observation channel is currently forwarding an observation from one entity to another. An active disturbance channel is currently triggering another disturbance channel or currently causing a physical disturbance in the user’s environment.

Related to a channel’s state is the *frequency* of activation, which is also motivated by the identified factors influencing users’ privacy con-
cerns (see Chapter 4). The frequency can be either onetime, recurring, continuous, or on demand.

A onetime channel is only active for a particular moment in a user’s activity. For instance an observation channel for which its content is forwarded only once or a disturbance channel causing a singular visual or acoustic notification.

Recurring channels are active for a specific time in fixed or dynamic intervals. For example, the observation channel of the fitness app in the running use case (Section 5.5.1) requesting the user’s position every 5 seconds. Or the disturbance channel of the coffee machine in the coming home use case (Section 5.5.3), which provides a notification every 30 minutes.

Continuous channels are always active. In case of observation channels they may contain dynamic or continuous data such as a video stream or other sensor data. A continuous disturbance channel, for instance, could be caused by the noise of the cleaning robot in the coming home case (Section 5.5.3).

Channels that are not active in a determined way can be activated on demand. This is especially relevant to model context-dependent channels. For example, to model the observation channel to the emergency service in the running use case (Section 5.5.1), which only gets activated in case of an emergency. Such context dependencies are specified as part of purpose statements.

**Protection** Optional information about a channel’s protection in terms of applied security mechanisms allows to determine the appropriate representation level for the model instantiation (see Section 6.2). While a channel protected via SSL does not need to be modeled at a higher detail level, an unprotected channel might cause several privacy implications, which would require a more detailed representation level and further discovery efforts. If the required detail level cannot be discovered, the model must be instantiated with uncertainty by modeling a channel to the unknown entity node (see Section 6.2).
Each channel specification provides a content part which describes the details of a privacy implication via a content category, a source or target type, an optional granularity description for observations, and optional details about applied protection mechanisms.

The content category provides a hierarchical description of the channel's content, see Figure 7.7. The categories for observations are motivated by P3P's [169] data categories in combination with Langheinrich’s [391] extensions for perception and location data categories and a taxonomy for data types in UbiComp by Price et al. [521]. Disturbance categories have been derived from related work on interruptions and automations in UbiComp, see Chapter 4 and Section 2.2.5.

In general, the content can be categorized into user and environment related content. User-related observations refer to direct observations as discussed in Section 5.3. Environment related observations (e.g., data from environmental light or humidity sensors, see Section 2.2.4) can result in indirect observations and therefore must be considered during the discovery process as well. User-related disturbances refer to interruptions of the user, that is direct disturbances that require a user’s attention and often cause a reaction or subsequent interaction.
Environment related disturbances are caused by noise in the environment that is not directed to the user.

Observations can further be static or dynamic. Static observations refer to personal data that remains unchanged (e.g., contact or demographic user information). Dynamic observations are either raw data from sensors (perception) and location sources, or are dynamically derived from other observations (e.g., the user’s activity from video and motion observations).

For instance, a video observation content would be described as:

\texttt{observation.user.dynamic.raw.perception.visual.video}

Disturbances are either of social or technical nature. Social user-directed disturbances refer to interruptions by messaging or conversations (e.g., mail, instant messaging, phone calls or video chats), and to the physical approaching of other persons. A phone call disturbance content would be described as:

\texttt{disturbance.user.social.conversation.phone-call}

Social disturbances in the environment may result from noise of conversations or others’ activities. Technical user-related interruptions can be caused by presenting information, notifications and warnings, or by the initiation of interactions. Automations that directly support a user’s current activity are also considered as user-related interruptions. Other automations or actuations in the environment are considered to be noise (e.g., from other persons’ mobile devices or automations of systems in public environments).

For observations, the content description can optionally provide details about the content’s granularity. While the granularity depends on the content type (e.g., resolution of a video stream or sampling rate of sensors), we assume the granularity to be provided as an abstract category of either low, medium, or high. This facilitates a simple presentation of privacy implications for supporting user’s awareness.

Finally, the content description can optionally inform about the content’s protection. Similar to the channel’s protection information, this allows to determine the required representation level during the discovery process. For instance, if the channel specification did not provide any protection details, but the content description informs that the content is encrypted for the source or sink entity, no higher detail level needs to be discovered. However, if no protection is specified or the content is encrypted for a different entity than the source or sink entity, the discovery process needs to perform further steps to assess the appropriate representation level.

\textbf{CONTROL POINTS} \hspace{1em} Available and authorized control points of a channel are specified in the same way as an entity’s control points, see Section 7.3.1. However, instead of controlling entity-specific functions, these control points allow to disable incoming or outgoing channels of an entity via control point references or control point interfaces.
7.3.3 Purpose statements

The last part of a channel policy is a set of one or more purpose statements, which are required to model the dependencies between different observations and disturbances for a specific purpose. Each purpose statement corresponds to one entity node of the privacy graph (see Section 6.1) and consists of a purpose description, one or more actions associated with specified channels, and purpose-specific control points, see Figure 7.8. An action can further be declared with optional conditions and obligations.

**PURPOSE DESCRIPTION** The purpose description informs about why an entity is affecting a user’s privacy. It consists of a purpose domain, the purpose target, and a purpose text. The domain is a custom label representing the high-level purpose category similar to P3P’s primary-purpose [169]. Examples of possible purpose domains are healthcare, entertainment, government, or communication. It is further possible to structure domains in a hierarchical order. This allows to specify more precise domains but at the same time supports abstraction levels, e.g., the healthcare purpose domain can have the subdomains health-monitoring or vital-assistance. Thus, domain descriptions can be easily extended. The idea of purpose hierarchies is also proposed by other privacy policy languages and access control models, see Section 7.2.

The purpose target defines what the current purpose pertains to. For example, if an entity is supporting the user or her activity, the purpose target would be user. This is similar to the semantic meaning of P3P’s current purpose [169]. However, P3P does not allow to explicitly specify a target. If an entity performs actions that support other entities, e.g., for marketing purposes, the corresponding entity would be declared as the purpose target. Thus, the purpose target allows to infer whether an entity is supporting the user or her activity, or some other entities.
Table 7.1: Possible actions and minimum number of associated incoming and outgoing channels declared in a purpose statement.

<table>
<thead>
<tr>
<th>action</th>
<th>incoming channels</th>
<th>outgoing channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>observation-related</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sense</td>
<td>$\geq 1$</td>
<td>$\geq 0$</td>
</tr>
<tr>
<td>forward</td>
<td>1</td>
<td>$\geq 1$</td>
</tr>
<tr>
<td>use</td>
<td>$\geq 1$</td>
<td>-</td>
</tr>
<tr>
<td>store</td>
<td>$\geq 1$</td>
<td>-</td>
</tr>
<tr>
<td>disturbance-related</td>
<td></td>
<td></td>
</tr>
<tr>
<td>act</td>
<td>$\geq 0$</td>
<td>$\geq 1$</td>
</tr>
<tr>
<td>trigger</td>
<td>$\geq 0$</td>
<td>$\geq 1$</td>
</tr>
<tr>
<td>control</td>
<td>$\geq 0$</td>
<td>$\geq 1$</td>
</tr>
</tbody>
</table>

The purpose text provides users a textual description that aids interpretation of the declared purpose, e.g., “The health app monitors your vital parameters and detects health critical situations”.

**Actions**  Actions provide information on how an entity handles observation and disturbance channels for a specific purpose. Through a literature review (see Section 3) in combination with the findings on users’ privacy concerns (see Chapter 4) and the features of the territorial privacy model (see Section 6.1), we identified a minimal set of seven actions deemed sufficient to represent different use and interrelations of channels. Table 7.1 lists these actions together with the minimum number of associated incoming and outgoing channels of the purpose statement that declares the corresponding action. Observation channel related actions are sense, forward, use, and store. Disturbance channel related actions are act, trigger, and control.

The sense action always indicates the source of an observation. It is associated with incoming observation channels of active observers (see Section 5.4.1). If this action is specified by a physical active observer, the associated channel is a physical observation and thus directly connected to the user as the source entity. Those entities can optionally specify an affected area as part of the sense action in order to allow the discovery process to determine if the user is being sensed at the current location. The affected area can either be specified relative to the entity’s location as provided in the entity description (see Section 7.3.1), or as an absolute area by a set of coordinates (e.g., specified in GeoJSON [123] format).

The forward action indicates that an entity’s incoming observation channel is forwarded to one or more other entities, which potentially could access the channel’s content.

A use action is declared for one or more incoming observation channels whenever an entity is accessing and processing the channel’s con-
tent (e.g., the user’s heart rate is analyzed). Similarly, the store action indicates that an entity stores a channel’s content.

Analogous to the sense action, the action act indicates the endpoint of a disturbance. It refers to outgoing physical disturbance channels of active disturbers (e.g., an acoustic signal of a speaker or the visual output of a display) that may be triggered by incoming disturbance channels. Optionally, an entity can specify the affected area of physical disturbances as part of this action similar to the sense action, and can also provide further details on the modality, presentation, and intensity of the disturbance. The modality can be a combination of acoustic, visual, or haptic. The presentation can be specified for user-related disturbances (e.g., notifications and information) and indicates how it is presented to the user (e.g., displaying, blinking, vibrating, or beeping). The intensity provides information to assess the intensity of disturbance. This information depends on the modality and presentation of a disturbance (e.g., volume of a beeping sound or brightness of a blinking LED) and is assumed to be mapped on abstract intensity levels of low, medium, and high.

The source of a disturbance is either indicated by a control or a trigger action. A control action is specified by an entity for an outgoing disturbance channel when it is able to directly control an active disturber or an entity which in turn triggers an active disturber. For instance, a home automation system controlling the blinds of the user’s room. A trigger action is declared by an entity for an outgoing disturbance channel when it creates events that cause disturbances (e.g., an application that triggers a warning). An active disturber can either be directly triggered or via multiple intermediate entities. For intermediate entities the trigger action has similar semantics for disturbances as the forward action for observations. The difference between trigger and control actions lies in their ability to control the type of disturbance. While a trigger action represents only an event without determining the type of disturbance (e.g., whether a warning is announced by an acoustic or visual signal), a control action is typically associated with a specific disturbance caused by the controlled entity (e.g., controlling the blinds of a room typically causes an audiovisual disturbance).

Each action can optionally have associated conditions and obligations similar to the access control approaches discussed in Section 7.2.

**Conditions** A condition specifies the required context dependencies that need to be fulfilled in order to perform this action. For instance, in the running use case (Section 5.5.1) the health state and location observation channels are only forwarded to the emergency service if the current health state is life-threatening. Thus, conditions provide a mechanism for specifying context-based privacy implications. The conditions of a sense, forward, and control action directly influence the state of associated channels. That is, a channel is only
active if the condition is fulfilled. Therefore, we assume that conditions can be evaluated to a Boolean value.

We propose two possible strategies to support this evaluation, either by context updates or evaluation updates. For context updates, a condition provides a reference to involved context parameters. This allows the privacy agent to register for context changes. The evaluation of the condition is then performed by the privacy agent each time a context change is received. For evaluation updates, a condition provides a reference which allows to register for evaluation changes, i.e., a condition becomes fulfilled or unfulfilled. Here the privacy agent does not need to perform the evaluation on its own. Both approaches could be realized via a central or distributed context provisioning middleware as discussed in Section 2.2.3. But because context parameters can also involve privacy-relevant observations (e.g., the user’s health state), a middleware approach might introduce further privacy implications. A privacy-friendly solution would be that entities provide evaluation updates whenever context parameters involve privacy relevant data.

**OBLIGATIONS** An obligation allows an entity to specify additional operations that will be performed before, during, and after a given action. This way an entity can provide detailed information about applied data handling practices and privacy mechanisms. For instance, an obligation could state for a forward action that an observation channel’s content is modified in order to anonymize it before forwarding (e.g., via blurring of faces in a video stream or obfuscation techniques for a user’s location). An obligation for a store action could declare how long an observation channel’s content will be retained and whether it is stored encrypted.

**CONTROL POINTS** An entity can optionally specify a set of control points in each purpose statement similar to the entity description (Section 7.3.1) and channel specifications (Section 7.3.2). These control points allow either to deny a complete purpose statement with all associated channels and actions, or to control specific actions with associated conditions and obligations. While the first type of control points only support a binary control decision similar to channel specific control points, the control of actions supports more fine granular privacy decisions. For instance, if the control point of an action allows to set or modify its associated conditions, a user can specify context-based privacy preferences which are enforced through the available control point. If automatic enforcement is supported, possible modifications of a condition or obligation are specified in the control point interface (see Section 7.3.1). The interface description of a control point for the forwarding action of the health state observation in the running use case could be declared as shown in Figure 7.9.
Figure 7.9: Control point interface for a forward action with six possible modifications of the associated condition.

The interface specifies six possible modifications of the associated condition. Thus, the condition for the forward action could be modified to respect the current health state (irregular or emergency), the symbolic location “at home”, the daytime “at night”, or a custom time slot. The last context “none” can be used to disable the condition for this action, resulting in an always active forwarding of the respective channel. A similar enumeration of modifications could be declared for obligations. For instance, a forward action for a location observation channel could provide different granularity levels of the location, such as coordinates, street level, or city level.

**EXAMPLE** An example to clarify the use of purpose statements with different actions is given in Figure 7.10. It depicts a partial instantiation of the privacy graph for the running use case as described in Section 5.5.1. The required channel policies for the graph instantiation show the different purpose statements of the four entities (e1 – e4) with corresponding observation channels o1 – o12 and disturbance channel d1. Actions of a purpose statement are donated as <action {channelSet}, condition, obligation>.

The user’s vital parameters are monitored by the health application e3 (on the user’s smartphone e2) via observation channels o4, o6, and o8 from the sensor wrist band e1. In case of a critical health state (condition) the user is warned through an acoustic signal (disturbance channel d1). Further, in case of an emergency the health state and current location are forwarded to the emergency service e4 in order to request first aid and to capture emergency statistics.

The purpose statement of the wrist band entity e1 specifies the purpose domain monitoring with the textual purpose description “provide vital parameters”. The purpose target remains unspecified. However, traversing the graph and collecting purpose dependencies as described in Section 6.4 allows to infer that this purpose serves the additional purposes of “warn on critical health state” and “request first aid” with target user, and the purpose “provide emergency stats” with target.
Thus, the “provide vital parameter” purpose does support the user on the one hand, but on the other hand does also support the emergency service. The same applies to the purpose of the smartphone’s GPS sensor $e_2$ “provide GPS position”. Both purpose statements of $e_1$ and $e_2$ specify the sense action for the logical observation channel $o_1$ and for the physical observation channels $o_4$, $o_6$, and $o_8$. For each of those channels a forward action is specified in combination with the channels $o_2$, $o_5$, $o_7$, and $o_9$, which forward the observations to the health app $e_3$.

The health app in turn specifies three purpose statements. The first statement “provide health state” refers to the virtual sensor capability of the health app, which derives the user’s health state from the incoming vital parameters. This is indicated by the use action associated with the vital parameter observation channels ($o_5$, $o_7$, and $o_9$), and by the sense action associated with the outgoing health state observation channels $o_{10}$ and $o_{11}$. The health state is used for conditional actions in both other purposes statements, in order to warn the user when the “health state is critical” (statement 2) and request first aid when the “health state is life threatening” (statement 3). These...
statements are modeled in the additional purpose nodes $e'_3$ and $e''_3$, respectively. Warning the user is indicated by the conditional action $act$ for disturbance channel $d_1$. Requesting first aid is indicated by the conditional $forward$ actions for the location channels ($o_2, o_3$) and health state channels ($o_{11}, o_{12}$).

Finally, the health service $e_4$ declares an obligation for the $store$ actions in its purpose statement. This indicates that the content of channels $o_3$ and $o_{12}$ (i.e., the user’s location and health state) are anonymized before being stored and will be deleted after one year.

### 7.4 Summary

In this chapter, we introduced the general discovery strategies for collecting channel policies and provided a specification of our proposed policy format. The different discovery strategies are influenced by features of the user’s current environment and can be divided into personal device discovery, infrastructure-based discovery, environmental discovery, and virtual remote discovery. Those strategies allow to discover privacy implications of entities in a user’s personal, physical, and virtual extended territory, respectively.

While there are several existing privacy policy languages, none of them provides all features required to represent the privacy implications of our territorial privacy model. Therefore, we proposed channel policies as a new container format which allows entities to specify their privacy implications and control points as required for the instantiation of our model. Thus, channel policies provide information about the entity, about an entity’s observation and disturbance channels together with associate purposes of observations and disturbances, as well as available control points.

The different discovery strategies to collect channel policies as well as the enforcement of privacy decisions based on available control points, is realized by different discovery and enforcement modules which will be discussed in the next chapter.
The previous chapters have introduced the territorial privacy model as well as the general discovery strategies of channel policies for its instantiation. The realization of these discovery strategies and the instantiation of the model is accomplished by a personal privacy agent (see Figure 8.1). The privacy agent is a software component which is deployed on a user’s trusted mobile device.

The main components of the privacy agent are discovery and enforcement modules, which are able to collect channel policies in different environments and support privacy enforcement based on available control points. We developed five distinct modules in order to cope with the heterogeneity of UbiComp systems, with their different privacy implications, and with the different settings and conditions of a user’s environment. The modules implement both optimistic and pessimistic approaches, in order to satisfy the different environmental requirements and assumptions.

A central privacy engine receives the channel policies from the different discovery modules in order to instantiate the privacy graph and to realize its application. The engine supports awareness of privacy im-

**Figure 8.1:** Overview of the privacy agent. The current environment influences the application of discovery and enforcement modules. The privacy engine instantiates and adapts the privacy graph and utilizes its features to support privacy awareness and control. Control can be exerted directly via the user interface or indirectly via user-defined privacy preferences.
applications via a user interface, which also enables a user to exert direct control or to specify privacy preferences. Those preferences are used by the privacy engine in order to automatically enforce privacy needs based on the current privacy graph (indirect control by a user).

In the following sections we first introduce the privacy engine followed by a detailed discussion of the different discovery and enforcement modules. The realization and evaluation of the user interface is discussed in Chapter 9.

8.1 Privacy Engine

The privacy engine is the central coordination component of the privacy agent and is responsible for performing three major tasks:

- instantiation and adaptation of the privacy graph
- strategy selection for privacy enforcement
- exception handling

We discuss each of these tasks in the following sections.

8.1.1 Privacy graph instantiation and adaptation

The privacy engine instantiates a new privacy graph whenever new channel policies are discovered by one of the discovery modules and no other privacy graph instance is currently active. This happens when the privacy agent is started or in situations in which new privacy implications emerge and no implications have been discovered before (e.g., when the user changes the own location or new entities appear in the user’s current environment).

In a similar manner the privacy agent adapts the privacy graph when context changes occur that affect the current instantiation (see also the discussion of discovery updates in Section 7.1) and whenever a new channel policy is discovered. The privacy engine further keeps a history of all graph instances and thus stores the current instance on every graph adaptation. In combination with the user interface (discussed in Chapter 9) the history allows users to gain awareness of all privacy implications in the past and therefore enables retrospection and later inspection of privacy implications. Thus, on the one hand it provides users with better awareness of privacy implications that might be difficult to perceive in real-time. Such implications could stem from systems that observe the user only in a short period of time (e.g., the surveillance cameras on the track in the running use case, see Section 5.5.1). On the other hand, it allows users to gain awareness of privacy implications that occurred in situations in which it was not possible or not desired to gain awareness instantly. The history
should further support users in the identification of potential privacy problems and in the formulation of new privacy preferences.

8.1.2 Strategy selection for privacy enforcement

The strategy selection for privacy enforcement is based on the mapping of a user’s privacy preferences or a user’s direct control decisions onto existing control points. This mapping is realized by the privacy engine through applying the privacy graph algorithms discussed in Section 6.4.2.

While a user’s direct control decisions are explicitly issued to the privacy engine through the user interface, indirect control decisions must be implicitly determined by a user’s privacy preferences. To realize this, privacy preferences must be associated with contextual conditions that specify when the particular preferences should be applied. The privacy engine validates the conditions and maps the preferences onto existing control points if the condition is met. For instance, the preference of Alice in the coming home use case (see Section 5.5.3) is “do not disturb when coming home from work.” Thus, the contextual conditions associated with her privacy preference are the time (weekdays, 18pm till 8am) and location (at home). We will discuss the definition of such preferences in Chapter 9.

8.1.3 Exception handling

Whenever the privacy engine is not able to determine an appropriate control strategy it is required to perform an exception handling procedure involving an explicit user decision. Such situations might occur when privacy control decisions can only be enforced with control points that also affect desired entities. Imagine the following situation for instance: A user does not want to be tracked through a shop’s WiFi tracking system. The privacy engine applies Algorithm 4 for enforcing undesired entity sets (see Section 6.4.2). Because the system does not provide any control points, the privacy engine identifies the smartphone’s WiFi module as the only available control point. However, switching off the WiFi module might also prevent other applications from accessing the Internet, which might have undesired consequences. In such a case, the privacy engine discovers those consequences (e.g., a health application cannot call for emergency) through the privacy graph and subsequently triggers the user interface to ask for a manual user decision.
8.1.4 Implementation

We\(^1\) implemented the privacy engine in Java and deployed it on an ordinary laptop. While the prototype platform only serves feasibility studies, using Java allows for an easy transfer of the engine’s implementation to Android as the target platform for the privacy agent. Channel policies and privacy preferences are represented and exchanged in XML format (see Appendix B for an example of a policy). Figure 8.2 provides an overview of the three main components of the engine’s implementation. The policy manager receives XML-based channel policies and translates them into policy objects. These policy objects can be used by the graph manager to instantiate the privacy graph with PrivacyNode and PrivacyEdge objects where the first refer to entities and the latter to associated observation and disturbance channels. The internal data structure of the graph was implemented using HashMaps. The interface connector provides access to graph information in order to support the user-level presentation of the graph through the user interface. Furthermore, the interface connector forwards control decisions containing desired or undesired sets of channels or entities to the graph manager. Based on these sets, the graph manager identifies appropriate control points in the graph with the algorithms described in Section 6.4.2. Control commands to identified control points are passed directly to the respective enforcement module, which subsequently might trigger policy updates. Possible conflicts are resolved by user involvement via the interface connector.

Performance evaluation

We evaluated the performance of the privacy engine through a simulation of an extended version of the coming home use case, see

\(^1\)The privacy engine has been implemented as part of the master’s thesis of Julia Greim [270].
Table 8.1: Performance results of the privacy engine for the instantiation of a privacy graph with 24 channel policies and for a best-case as well as a worst-case control decision.

<table>
<thead>
<tr>
<th></th>
<th>instantiation</th>
<th>best-case control decision</th>
<th>worst-case control decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>∅</td>
<td>156.69ms</td>
<td>0.29ms</td>
<td>12.84ms</td>
</tr>
<tr>
<td>σ</td>
<td>5.89ms</td>
<td>0.06ms</td>
<td>1.31ms</td>
</tr>
</tbody>
</table>

Section 5.5.3. The scenario was extended with further entities on the user’s smartphone and further remote entities in order to form a more complex use case for the performance evaluation. In total, the scenario involved 24 entities with respective channel policies. The simulation consisted of the initial graph instantiation and the identification of control points for two different control decisions. The instantiation involved the parsing of XML-based channel policies and the creation of the graph’s data structure. Note, that the discovery process was not part of the benchmark. The identification of control points involved a best-case control decision without the need of a graph traversal and a worst-case control decision in which the graph must be traversed back over 6 channels in order to identify the adequate control point. We utilized Java’s management interface for monitoring the Java virtual machine and measured the total CPU time as the amount of ThreadCpuTime plus ThreadUserTime. The tests were conducted on a Linux machine (Kernel 3.13.0-24) with an Intel Core 2 Duo CPU with 2.4GHz. We ran each test 50 times and calculated the mean CPU times. The results are shown in Table 8.1, which highlight the acceptable performance of the privacy engine for our use case. While the results only reflect the performance of the privacy engine, the instantiation time of the privacy graph will be further influenced by the discovery process of channel policies, especially of remote entities, which might cause longer delays.

8.1.5 Discussion

As the heart of the privacy agent, the privacy engine performs the essential tasks for managing a user’s privacy through graph based operations based on the territorial privacy model. Our prototype implementation showed the feasibility of our approach and its reasonable performance for an extended version of the coming home use case. However, the feasibility and effectiveness in a real world scenario strongly depends on the provisioning of channel policies from the different discovery and enforcement modules that we will discuss in the following sections.
Figure 8.3: Integration and main functionality of the personal device module. It supports the registration of personal devices and observable items, and enables the discovery of channel policies and the enforcement of privacy decisions in the local application framework of the privacy agent’s host device, i.e. the user’s smartphone.

8.2 PERSONAL DEVICE MODULE

The main objectives of the personal device module are the registration of a user’s observable items (see Section 5.3), the discovery of logical and physical channels (see Section 6.2.2) of a user’s personal and wearable devices, and the control of those devices according to privacy decisions. Personal devices could also involve several subentities, e.g., in form of mobile applications, which need to be respected in the discovery and enforcement process. Figure 8.3 shows a high-level view of the personal device module’s integration and functionalities as part of the privacy agent and of the smartphone’s application framework in form of a privacy enforcement layer.

8.2.1 Registration of devices and observable items

Whenever a user is wearing, carrying or using a personal device or observable item in direct proximity, it must be registered with the privacy agent. The registration can either be performed automatically or manually. Automatic registration can be applied for all devices and items that communicate with the privacy agent’s host, i.e., the user’s smartphone. For instance, a smart watch, a sensor wrist band, or even the user’s car. The personal device module collects any available channel policies as part of the connection establishment and stores observable IDs. For instance, devices connected via Bluetooth can provide
their channel policies as part of the service discovery protocol (SDP) in a Bluetooth profile.

Observable IDs allow to identify a user’s devices or items based on unique identifiers of their wireless communication technologies and underlying protocols. For instance, such an identifier can be the IMSI number of a GSM cellphone, or the MAC address of a Bluetooth or WiFi module on the user’s smartphone or smartwatch. An observable ID is specified as the concatenation of the technology or protocol with the respective identifier, e.g., WIFI|90:4c:e5:1b:63:2b for an observable ID referring to the MAC address of a WiFi module).

In order to register observable IDs, they can either be explicitly integrated in channel policies of personal devices, or they can be implicitly determined by the personal device module through the established connection. For instance, the Bluetooth stack of the host device could pass the MAC addresses of connected devices to the personal device module. If a device or item is not connected to a user’s smartphone (e.g., an independent wearable device), it must be registered manually. We propose to leverage a single interaction method for this purpose based on NFC or QR-code scanning, which allows to receive channel policies and observable IDs. Here, a scanned NFC tag or QR-code could provide a reference to the respective channel policies.

For each discovered observable ID, the personal device module creates a logical location observation channel (see Section 6.2.2) to the respective device or item. This allows to model observation channels that occur from environmental sensors that are able to detect the presence of a user’s device and thus can infer a user’s location. In order to allow the correct mapping of such an observation channel, those observable item detectors (see Section 5.4.1) are required to either provide the observable item’s entity identifier, one of the item’s observable IDs, or at least the type of the detected wireless technology in their channel policies. While providing the entity identifier or an observable ID is applicable in an authorized discovery process, providing the wireless technology type can also be applied in an anonymous discovery process. For instance, when an observable item detector only indicates WIFI as the source technology for a location observation channel, the personal device module must connect this logical observation channel to all personal devices and items with associated WiFi-based observable IDs. This can be achieved by modifying the channel policies of observable item detectors before they are passed to the privacy engine.

Note that the host device of the privacy agent itself may be equipped with several communication modules and thus is also an observable item on its own. Therefore, observable IDs of existing communication modules are also registered through the personal device module based on their current state.
### 8.2.2 Local application framework

A part of the personal device module is integrated in the local application framework of the privacy agent’s host. This allows to discover channel policies from local applications and to control privacy decisions through a *privacy enforcement layer*. Channel policies of applications can be discovered via an optimistic or pessimistic strategy.

The optimistic strategy assumes that applications provide their channel policies at install time and when being started. If an application does not provide a local channel policy, it can alternatively be fetched from a central policy database. This database can either be populated by application developers or by third parties who create policies based on analyzing existing apps for privacy implications similar to the approach proposed by Rosen et al. [546]. The idea of a central policy database will be further discussed as part of the community-based discovery module in Section 8.5.

For the pessimistic strategy it is assumed that no channel policies can be discovered either locally or via the remote policy database. In order to still provide basic information for the model instantiation, the privacy enforcement layer monitors each access of an application to a device’s sensors, actuators, and communication modules. The resulting access log is used to create and update channel policies, which are passed to the privacy engine for each application that does not provide a policy on its own. The monitoring approach can also be leveraged to detect malformed policies from applications, which then can be updated in the central database.

In order to enforce privacy decisions, the privacy engine identifies appropriate control points, which are then used by the personal device module. These control points are either *application-specific* (e.g., to control a conditional purpose of an app), or *framework-specific* (e.g., to control channels from sensors or channels to actuators). While the first type of control points requires the collaboration of applications that are assumed to be trusted, the latter type of control points can be used also for untrusted applications to enforce privacy decisions without their collaboration. For instance, by denying access to the GPS sensor, providing the location on a lower detail level, or limiting the frequency of a forwarding channel by controlling access to communication modules.

### 8.2.3 Implementation

We implemented the privacy enforcement layer as part of our open source *Ginger* framework. We provide a detailed description of the Ginger framework in [9].

---

2 Ginger has been jointly developed as part of the diploma thesis of David Herges [299]. The source code can be accessed via: https://gitorious.org/ginger/
Table 8.2: Performance results for framework-specific privacy enforcement via control points for setting a location granularity obligation (left) and setting a forwarding frequency obligation (right).

<table>
<thead>
<tr>
<th>Location Granularity</th>
<th>AOSP</th>
<th>Ginger Factor</th>
<th>Forwarding Frequency</th>
<th>AOSP</th>
<th>Ginger Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>∅</td>
<td>29.86ms</td>
<td>34.88ms 1.17</td>
<td>∅</td>
<td>2.16ms</td>
<td>9.54ms 4.42</td>
</tr>
<tr>
<td>σ</td>
<td>15.47ms</td>
<td>14.12ms 0.91</td>
<td>σ</td>
<td>4.44ms</td>
<td>4.56ms 1.03</td>
</tr>
</tbody>
</table>

Ginger is based on a modified version of the Android Open Source Project (AOSP). In order to integrate the privacy enforcement layer in Android’s application framework, we modified the Binder IPC (a synchronous inter-process communication mechanism based on shared memory) and several system APIs to allow the monitoring and access management of sensors, actuators and communication modules. The enforcement layer provides a system-level message service which forwards discovered channel policies to the privacy engine.

Performance evaluation

In order to assess the efficiency of our Ginger implementation, we conducted a performance evaluation compared to the AOSP baseline version. The evaluation was conducted with an Android emulator running on an OS X 10.7.3 machine, 2.26 GHz Intel Core 2 Duo.

We implemented a demo application that provides a similar functionality as the fitness app described in the running use case (see Section 5.5.1). The GPS location was accessed every second and forwarded to the fitness service. For the evaluation we assumed the pessimistic scenario. That is, the fitness app neither provided channel policies nor control points. Therefore, framework-specific control points were required to enforce a user’s privacy preferences, which were defined as “grant access to location in mid-level granularity and limit location forwarding to once in a minute.” These preferences were mapped onto the application framework’s control points in order to set obligations for the GPS sensor and communication modules.

We let the demo application repeatedly (n=1,000) receive location data and transmit network data, while measuring time instances for each operation. Mean timing results are provided in Table 8.2. They show that location access causes an overhead of about 5ms for Ginger, due to the evaluation of channel policies and privacy preferences, and the enforcement of the location granularity obligation via the framework’s control point. Controlling the forwarding frequency of the location causes an overhead of about 7.4ms. While the overhead of both enforcement strategies is acceptable, the slightly higher overhead of controlling the forwarding frequency might be caused by the

---

3 AOSP v2.3.7r.1, https://source.android.com/
4 At the time of the evaluation the AOSP baseline version was Gingerbread v2.3.7_r1
fact that controlling access to the communication modules requires an additional IPC operation in Ginger compared to a native library call in Android. However, this could be further improved by implementing the required functionality in native libraries.

8.2.4 Discussion

The personal device module is responsible for the registration of observable items, the discovery of channel policies from personal devices, and the enforcement of privacy preferences on those devices. With respect to our introduced use cases (see Section 5.5), the personal device module is required for several purposes. In the running and coming home use cases it registers Alice’s smartphone and wrist band as personal devices and receives involved channel policies. Those are the channel policy of the wrist band, the policy of the fitness app, the policy of the health app, and the policy of the phone call app. Those policies in turn reference the channel policies of the involved remote entities. In the working and coming home use cases, the personal device module is further required to register Alice’s smartphone as an observable item, which allows to associate a location observation channel with the WiFi detector.

For untrusted applications or applications that do not provide any control points, the personal device module supports privacy enforcement by integrating a privacy enforcement layer in the application framework of a user’s personal device. The prototype implementation showed the feasibility of the enforcement layer when deployed on the same device as the privacy agent. However, a similar enforcement layer could be integrated on other personal devices in order to provide an interface to the privacy agent.

8.2.5 Related work

There are several approaches related to the local application framework of the personal device module that focus on enhancing privacy on user’s smartphones. AppFence [309] is a privacy framework for Android which allows to block network transmissions that contain data flagged for on-device usage only. AppFence is able to transparently substitute shadow data in place of private data. The data labeling relies on the information-flow tracking system TaintDroid [214]. Similar to Ginger, TaintDroid is based on a modified version of the AOSP.

Berthome et al. [92] propose a solution for automatic access detection and monitoring without requiring any modification to the operating system. Their approach is based on repackaging applications with injected bytecode of a monitoring component which reports access to sensitive resources. A similar monitoring approach is realized in AppGuard [65], a commercial Android application which allows
a user to browse the access history of installed applications and to specify policies to prevent undesired access.

Rosen et al. [546] propose to analyze the privacy implications of applications offline in order to create a central knowledge base. This know that can be requested when installing a new application.

The Apex framework [470] allows users to specify run-time constraints for individual application permissions. After installation of an application, a policy configuration tool allows users to grant, deny, or conditionally grant individual application permissions (e.g., “let the application send a maximum of 5 text messages per day”).

The projects Protect My Privacy (PMP) [37] and XPrivacy [423] propose to combine monitoring and enforcement strategies with a crowdsourced recommendation approach. A central database collects privacy settings and preferences of users and provides the most common settings as a recommendation when installing new applications.

8.3 TRUSTED ENVIRONMENT MODULE

The trusted environment module supports discovery of channel policies and enforcement of privacy preferences in trusted environments with a closed and secured infrastructure. This typically can be assumed in personal, shared personal, and sometimes in shared environments (see Section 5.1).

Figure 8.4 illustrates the general functionality of the module. Discovery and control is either directly supported via the infrastructure or indirectly supported via a trusted system as the central control unit of the infrastructure together with existing sensors, actuators, and output devices. For instance, infrastructure based discovery and control can be realized in (wireless) local area networks at home in combination with UPnP [660] when devices are located in the same network as the privacy agent. However, UbiComp systems or existing home automation systems often utilize several heterogeneous networks (e.g., ZigBee [710] or power line networks) in order to connect a multitude of different devices. Therefore, such systems are required to provide indirect discovery and control capabilities to the privacy agent in a trusted manner.

Our development of the trusted environment module was realized as part of the EU-funded project ATRACO,5 which aimed at creating a trusted system for ambient intelligent environments. After briefly introducing the notion of trust and technical mechanisms for trust establishment, we will discuss the main components of an ATRACO trusted system, followed by a detailed discussion of the functionality and implementation of the trusted environment module. For further details we refer to our previous publications on privacy and trust management in ATRACO [4, 5].

5 Adaptive and Trusted Ambient Ecologies: http://www.uni-ulm.de/in/atraco
Although trust is a common social concept it is relatively difficult to define concisely. Like privacy, the term trust has a huge definitional diversity, which often leads to more confusion than to a better understanding of the term. As a consequence, some researchers argue that their “purposes may be better served . . . if they focus on specific components of trust rather than the generalized case” [447].

Nevertheless, there is a set of trust properties, which are commonly recognized among most trust researchers in the context of information technologies. They agree that trust is subjective, asymmetric, context- and situation-dependent, dynamic and non-monotonic, and typically not transitive [22, 137, 435, 654].

Some of these properties are reflected in one of the most adopted trust definitions formulated by Gambetta [246]: “trust is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action . . . and in a context in which it affects his own action.”

Depending on the environment in which trust is specified, it can be considered as a composition of different attributes like reliability, dependability, honesty, truthfulness, security, competence, and timeliness. Utilizing these attributes, Grandison and Sloman [266] define trust as “the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context.”

Chopra and Wallace [153] tried to find a common denominator of various definitions and argued that an integrated definition of trust consists of at least three elements. A trustee to whom trust is directed, confidence that the trust will be upheld, and a willingness to act on that confidence. Based on these elements they define trust as “the
willingness to rely on a specific other, based on confidence that one’s trust will lead to positive outcomes.”

Further, trustworthiness of an entity can be interpreted as a level of trust, that could be established over time by monitored information. Therefore, “trust can be seen as a complex predictor of the entity’s future behavior based on past evidence” [581].

Although the given definitions do not explicitly use the term risk in their formulation, the inclusion of risk is implied by most definitions in terms of uncertainty and negative outcomes if trust assessment fails. Thus, while most researchers agree that trust is inherently related to risk, it remains challenging to formulate a precise relation between the two notions [420, 603].

In the context of information technology and UbiComp in particular, one can differentiate between technical trust and social trust. Technical trust refers to trust in system components and devices with respect to their intended functionality, reliability, and safety. Social trust refers to the way human beings perceive and understand the notion of trust in social interactions and social relationships. This form of trust needs to be respected whenever a system component is involved in multi-user situations.

Trust establishment

Technical trust establishment is often based on the concept of computational trust. Existing mechanisms and models for computational trust can be classified into credential-based and reputation-based mechanisms [369, 555].

Credential-based computational trust refers to cryptographic solutions for establishing trust by obtaining and verifying credentials of an entity. These credentials are usually issued in form of digital certificates by a trusted third party or certificate authority (CA). This approach is commonly used to authenticate identities or memberships in Internet applications, often based on public key infrastructures (PKIs) [250, 514]. A PKI is an infrastructure for public key management and for the issuance of digital certificates. The main part of a PKI is a hierarchical arrangement of digitally-signed certificates for assuring bindings of public keys or attributes to specific identities.

Based on this notion of trust, Blaze et al. [102] introduced the term trust management, which involves the formulation of policies and credentials, determining satisfaction of credentials to policies and deferring trust to third parties.

Despite certain shortcomings of PKIs [211], this approach allows an initial binary trust assignment, which can support the decision if a component or device should be used or not in a given context.

In social interactions, trust can be established based on personal assessments, experience or reputation. Reputation-based trust establishment uses the history of an entity’s past behavior or recommen-
dations and experiences about this entity provided by other entities to compute a certain trust level [334]. Well known applications for reputation-based systems are electronic markets like eBay or Amazon, where buyers rate the reliability of sellers and merchants [334]. The main challenge here is to find adequate trust metrics and models to support this kind of computation. One of the first attempts at formalizing such trust metrics was made by Marsh [435]. His model was based on linear equations and was further extended by Abdul-Rahman and Hailes [22] to address trust in virtual communities.

Other approaches for the computation of trust and reputation values are based on the use of probability theory [571], fuzzy logic [135], or the use of entropy [595]. Similar models have been adopted by distributed mechanisms for computing reputation values in peer-to-peer networks [23, 700, 609].

### 8.3.2 ATRACO trusted system

The main objective of the ATRACO project was to realize a trusted smart home system, which is able to support users in their daily activities and tasks at home by autonomously adapting resources and system behavior according to contextual changes and user preferences.

ATRACO uses a service-oriented architecture (SOA) at the resource and system level to support numerous devices, sensors, and ubiquitous computing applications. Several agents complement the SOA infrastructure by providing high-level adaptation to a user’s task. ATRACO agents support adaptive planning, task realization and enhanced human computer interaction. The concept of ontologies is used to address the semantic heterogeneity that arises in smart environments. Ontologies provide a common repository of system knowledge, policies and state.

The instantiation of agents to support a specific user task is based on the concept of activity spheres. An activity sphere is the utilization of knowledge, devices, services and other resources required to realize an individual user goal within ATRACO.

From a privacy point of view, the main components of the ATRACO architecture are the sphere manager, the ontology manager, the interaction agent, the trust manager, and the privacy manager as depicted in Figure 8.4. We will briefly describe the functionality of each component in the following. A more detailed discussion of the ATRACO core concepts and architecture is given by Kameas et al. [338] and in the book “Next Generation Intelligent Environments” [295], which provides an overview of the objectives and outcomes of ATRACO. Our contribution to the project was the design and integration of the trust and privacy manager components.
SPHERE MANAGER The sphere manager is responsible for initializing or dissolving an activity sphere with its associated resources. Software and hardware resources are discovered and controlled by the sphere manager via a UPnP-based middleware that abstracts from different underlying heterogeneous home automation infrastructures and software frameworks. Resource discovery and selection is supported by computational trust assessments of the trust manager.

The sphere manager acts as an event service to other components of the activity sphere, e.g., it notifies the privacy manager of privacy-relevant context changes such as the appearance of other persons. The location of persons is determined in ATRACO by an ultra-wideband indoor tracking system, which allows to locate a person with high precision of less than a meter. Therefore, it is assumed that every user is equipped with a unique ultra-wideband batch, which also supports authorization.

Further, the sphere manager monitors the execution of the task workflow and adapts the composition of resources in case of any conflicts, such as failing devices, trust issues, or other exceptions.

ONTOSTY MANAGER AND ONTOLOGIES The ontology manager is responsible for managing the central knowledge base for an activity sphere, which is composed of different ontologies. The main sphere ontology is formed by merging or aligning more specific domain ontologies, task ontologies, and an upper level ontology, which describes basic entities and relationships in ATRACO. The sphere ontology also provides the required information to enable the indirect discovery of involved channel policies. A user profile ontology contains user preferences, user properties and other personal related information. It also provides an individual’s privacy preferences.

INTERACTION AGENT The interaction agent offers multimodal services to interact with the user and provides an interface to the system. In order to provide smooth interaction the interaction agent uses distributed multimodal interaction widgets which adapt to the user’s context. Therefore, the user interaction can be distributed among available modalities and devices at runtime, for instance to enforce privacy preferences in multi-user situations.

TRUST MANAGER The trust manager assesses the technical trustworthiness of devices and system components in terms of their reliability, compatibility, and intended functioning. A trust assessment is requested by the sphere manager whenever a new activity sphere is started or a new component appears in an already running activity sphere to support the decision of resource composition.

We propose to combine credential-based mechanisms for trust assessment with reputation-based mechanisms. The first is based on
signed device and service descriptions that are discovered via UPnP. Those descriptions should provide a digital certificate (or reference to the certificate) of this entity as well as generic channel policies. A digital certificate should be issued by an ATRACO certificate authority and confirms the validity of a component’s properties, such as an identifier, the manufacturer, type, and a serial number. Verifying the certificate and the associated device or service description does either result in a trusted, untrusted or unknown state for the component.

While untrusted components are excluded from an activity sphere, trusted and unknown components can be assessed by reputation-based mechanisms. The operations and interactions of those components are continuously monitored to dynamically assess the component’s proper functioning and reliability. Monitoring results are stored in a central database in order to collaboratively collect and receive monitored information about a specific component.

In multi-user situations of an activity sphere, the trust manager supports privacy protection and access control of user interfaces with social trust assessments. We adopted the concept of trust groups in order to address the problem of defining specific trust levels, which are typically difficult to determine computationally for other persons [390]. Trust groups represent groups of individuals with the same level of assigned trust (e.g., family, friends, or colleagues) and provide an adequate abstraction layer for user-oriented inter-personal trust management. By default, a trust group will not have assigned a specific trust level. Trust will be implied by specifying access policies either for personal information that utilize trust for privacy protection, or for control instances of systems in a personal environment. For example, a smart home system that controls the heating or light levels should be accessible only by family members.
Figure 8.5 shows an arrangement of trust groups and access control policies, which are provided as ontologies by the ontology manager. In order to ease the management of access control policies, controls are organized in different control domains, such as environment controls or entertainment controls. In a similar way, sensitive information items can be organized in different categories, for instance demographic information or personal pictures. Those categories are aligned to the content categories of observations discussed in Section 7.3.2.

To enforce such access control policies, the trust manager receives location events of present persons from the sphere manager. In addition, the interaction agent registers each user interface belonging to a specific control domain with the trust manager. Thus, the trust manager always knows the location of each user interface and can lock or unlock it depending on persons’ locations and social trust settings. For instance, if Charlie (as depicted in Figure 8.5) is in physical range of the heating control, the trust manager will lock it because Charlie is denied access to environment controls.

8.3.3 Privacy management

The trusted environment module supports the direct discovery of channel policies and the direct control of components according to privacy preferences through the UPnP-based infrastructure. This assumes that components provide their channel policies as part of their UPnP device and service descriptions. Available privacy control points are provided as mappings onto a component’s UPnP control points.
Direct discovery and control is required for autonomous components that are not part of a higher level trusted system. For instance, the cleaning robot of the coming home use case (see Section 5.5.3) could be part of the trusted home infrastructure, but not part of the trusted smart home system.

Indirect discovery and control is supported by the trusted environment module through the trusted system. Indirect discovery is realized in combination with the ontology manager of the trusted system, which automatically forwards the set of relevant channel policies to the trusted environment module. Indirect control is realized by the trusted environment module through setting and updating a privacy policy ontology (PPO), which reflects a user’s privacy preferences. Thus, the enforcement of privacy preferences is delegated to the trusted system’s privacy manager, which controls system components according to the PPO.

Initial privacy preferences are provided by the privacy agent and can be modified via a web-based ATRACO personal control interface, which applies necessary updates to the PPO. The control interface does further allow to modify trust groups and access rules to existing control interfaces if the current user has administration privileges. Figure 8.6 shows a screenshot of the trust group management interface. The interfaces for managing access to environmental controls (e.g., light control or heating control) and for updating a PPO related to personal photos are depicted in Figure 8.7.

Privacy Policy Ontology

In an ATRACO trusted system, a Privacy Policy Ontology (PPO) describes how and under which conditions an entity is allowed or not allowed to handle observations or to cause disturbances in an activity sphere according to a user’s privacy preferences.

The key attributes of a PPO are aligned to the information in channel policies (see Section 7.3) in order to allow a mapping of user preferences onto available control points. Thus, they provide information about the allowed entity, channel type (observation, disturbance), content type (e.g., static information, sensor data, or kind of disturbance), purpose, actions (e.g., store or forward), obligations (e.g., retention), and conditions (e.g., location or time).

Figure 8.8 shows a simplified example of an PPO, granting family members access to view vacation pictures for a time period of one year for the purpose of a slideshow.

Privacy enforcement

The privacy manager serves as a privacy interface for other components in the ATRACO architecture. Whenever a privacy-relevant event occurs, such as a context change or the initiation of a new ob-
8.3 TRUSTED ENVIRONMENT MODULE

Figure 8.7: Screenshots of the web-based ATRACO control interface for managing access to environmental controls (top) and a privacy preference management for personal photos (bottom).

...servation or disturbance channel, the privacy manager requests related policies and contextual information from the ontology manager. Based on a subsequent policy reasoning process the privacy manager enforces privacy by granting or denying access requests or by adapting current components of the activity sphere. If any conflict occurs during the reasoning process, the privacy manager can trigger the interaction agent in order to ask the user for a conflict resolution, such as modifying policies or adding policy exceptions. We will outline the interplay of different components for privacy enforcement, along with a discussion of potential privacy-affecting events.

- **initiation of observation channels:** New observation channels are initiated by the trusted system when personal information is requested from the ontology manager or when environmental sensors are being activated. When personal information is requested, the ontology manager triggers a PPO validation, which involves the requesting entity and the current context.
A special case occurs whenever the interaction agent requests personal information. The privacy manager then checks if any other persons are located inside the user’s physical territory by querying the ontology manager. If this is the case, the privacy manager uses the interaction ontology to determine the intended presentation modality for the information and whether it is accessible by other persons. If it is accessible by others, for example a large screen display, the privacy manager revalidates the PPO with respect to present persons. On a deny decision, the privacy manager either retains the personal information or adapts the interaction modalities of the interaction agent to ensure that unauthorized access to personal information is prevented, e.g., by presenting it on a user’s mobile device.

When the sphere manager requires sensor data for the realization of an activity sphere, it decides to activate a specific sensor after having received the trust validation of the trust manager as described in the Section 8.3.2. The activation for the sensor must be granted by the privacy manager, which performs the same PPO validation as described before.

- **initiation of disturbance channels**: New disturbance channels are initiated when actuators are going to be started or when the interaction agent is triggered. Therefore, the privacy manager performs similar privacy validation steps when the sphere manager is going to utilize actuators for the realization of an activity sphere or when the interaction agent is going to produce outputs or wants to initiate an interaction. Validation results for actuators either grant or deny the use in the current activity sphere. For the interaction agent, the results could deny the complete interaction or deny only some modalities, e.g., deny sound but allow visual output.

- **context changes**: Contextual changes, such as an activity change, a location change or appearing persons, are reflected as events by the sphere manager. Whenever such an event occurs, the privacy manager performs appropriate privacy validation steps.
In the case of a newly appearing person, the privacy manager checks whether personal information is currently presented by any interaction modality the new person would have access to. This information is obtained either from the interaction ontology or directly from the interaction agent. If so, the privacy manager may again adapt the interaction modalities based on the policy reasoning results of the PPO, as described above.

In case of activity or location changes, the privacy manager checks if any device or remote entity is currently observing or disturbing the user in his new territory. If so the privacy manager performs a PPO validation and, based on the results, excludes undesired observing and disturbing entities by switching off relevant sensors or active devices, respectively.

### 8.3.4 Evaluation

A prototype of the ATRACO architecture has been deployed and evaluated at the University of Essex in its iSpace laboratory, a real world testbed for home technology, see Figure 8.9. An evaluation of the ATRACO privacy components was performed as part of a scenario-driven user study. The scenario consisted of five parts demonstrating different features of the ATRACO prototype. After a short introduction to the iSpace, participants experienced the different scenario parts imagining that the iSpace was their home. Each scenario part was followed by a short interview in which participants were asked about their perceived appropriateness of system adaptations as well as about their overall experience and satisfaction.

In total, nine participants (5 female, 4 male) attended the user study. While most (7) participants were between 22 and 35 years old, one was between 36 and 49, and one was older than 50 years. In the following we describe the privacy-relevant parts of the scenario followed by a discussion of the qualitative results. For a description of the other scenario parts not pertaining to privacy we refer to [297].
Scenario

Alice arrives at home after work. She unlocks the front door by holding an RFID tag to the reader and enters the hallway (see Figure 8.9). She walks into the living room towards the main couch. The ATRACO system asks Alice to adjust the lights. She sits down on the sofa and adjusts the lights through the ATRACO interface on the tablet PC.

As she is sitting on the couch, the ATRACO system asks Alice if she wants to look at holiday pictures on the main screen. Alice accepts and the slideshow starts (see Figure 8.10 a). After a while her roommate Bob enters the room. His presence is automatically detected and the privacy manager starts a privacy reasoning process about Alice’s privacy preferences, which may result in the system’s decision that Bob should not see some of the pictures. If the access is denied only to some pictures, the privacy manager will seamlessly exclude those pictures from the slideshow. If the complete slideshow is private, it is stopped by the privacy manager as shown in Figure 8.10 b). In this case, Alice can manually resume the slideshow to implicitly grant Bob access to the pictures (see Figure 8.10 c).

A similar privacy adaptation approach has been employed in a computer-centric office scenario. If Bob approaches Alice while she is doing sensitive office work (e.g., online banking), the privacy manager can dynamically hide the sensitive parts on her screen.

User reactions

The service of automatically hiding private information in presence of other persons was generally accepted by the participants. However, the approach of explicitly hiding sensitive information (e.g., the complete slideshow instead of some pictures) revealed the issue that direct adaptation makes Bob aware of Alice’s privacy preferences concerning himself. This could potentially cause social tensions.

In general system interactions participants were concerned about the ability to control the system’s autonomous processes. In situations where the user felt out of control, reactions to the system were mostly negative. Especially in situations when the system initiated undesired
interactions that were perceived as an invasion of personal space. For example, when the system asked participants whether they would like to listen to music or look at photos as soon as they arrived at home. In some cases, participants were comfortable with the system initiating interactions, such as when the system announced a guest arrival at the front door. Perceptions of control may also be influenced by the channel of interaction. Voice interactions appeared to imply the existence of a separate social presence, which could lead to a feeling that the personal space has been invaded. Also mood changes could have an impact on the way a user prefers to interact with the system.

8.3.5 Discussion

The trusted environment module allows for direct and indirect privacy discovery and control in trusted environments. While direct discovery and control through UPnP only requires a trusted infrastructure, indirect discovery and control assumes that privacy management can be delegated to a central component of a trusted system. We discussed the ATRACO system as an implementation of such a trusted system for smart home environments.

With respect to privacy enforcement, direct control via the trusted UPnP infrastructure is best suited for spontaneous privacy decisions that are not represented in privacy preferences. In the coming home use case (Section 5.5.3) direct control could be applied to stop disturbances from the cleaning robot and the coffee machine. However, for more static privacy decisions that can be represented in form of privacy preferences, the indirect (delegated) control approach is preferable as it does not require the involvement of the privacy agent for every single privacy decision. In the coming home use case this requires the smart home system to be a trusted system in terms of the ATRACO approach. Privacy preferences can than be stored in the PPO, for example to specify access rules for the door opener, access rules to Alice’s location, or to specify conditions limiting the activity recognition functionality of the smart home system.

The results of the ATRACO evaluation show the technical feasibility of the trusted environment module for enforcing access to sensitive information. The results also highlight that privacy concerns of participants in UbiComp environments often involve territorial privacy aspects, such as the fear of losing control and the perception of privacy invasion through undesired forms of autonomous interactions. While the trusted environment module in principle addresses these aspects as well, the privacy preferences for the evaluation scenario have been statically configured and thus did not reflect participants’ individual preferences towards undesired disturbances. Thus, further studies would be required to demonstrate the modules’ feasibility to cope with undesired disturbances as well.
8.3.6 Related work

As related work on trust in UbiComp has already been discussed in Section 8.3.1 and further privacy frameworks for trusted environments have been presented in Section 3.5.3, we will limit our discussion in this section to only the most related approaches with respect to the ATRACO trusted system.

A trusted domain platform for trust establishment in home automation has been proposed by Hjorth and Torbensen [303]. Similar to ATRACO, the platform dynamically and securely connects several heterogeneous wireless networks and manages access control to home automation devices.

Bagüés et al. [67] propose Sentry@HOME as a privacy proxy similar to the ATRACO privacy manager. The proxy is part of a user-centric privacy framework based on a trusted home infrastructure and controls access to all privacy-relevant data. Policies are also represented in form of ontologies in order to support efficient reasoning.

A trusted infrastructure for privacy protection in smart environments with pervasive sensors is also assumed by Gong et al. [256]. Similar to ATRACO they propose tracking of users’ wireless batches in order to support dynamic location based privacy adaptation. Privacy preferences for video and audio sensors at different locations are preconfigured via a web-based interface to support automatic adaptation. Further, users can manually control privacy via on/off switches of devices and via a blocking button on the batch, which allows immediate privacy.

We also contributed to the PriCal system proposed by Schaub et al. [11]. PriCal is an ambient privacy adaptive calendar display which respects preconfigured privacy preferences for calendars and dynamically adapts the display according to present persons. In contrast to ATRACO, we realized PriCal as a decentralized system which does not track users, but only detects their presence in proximity of a calendar display. However, a trusted infrastructure in form of each single calendar display is also assumed in this approach, because displays receive and handle user’s personal schedules.

8.4 beacon-based discovery module

The personal device module as well as the trusted environment module are based on the assumption that privacy-affecting entities either exist on or in form of personal devices or are part of a trusted infrastructure to which the privacy agent has access. While this assumption often can be made in personal or shared personal environments, it does not hold for shared and public environments (e.g., offices, shopping malls or public places). In those environments, privacy-affecting entities can be part of several independent systems (e.g., autonomous
8.4 beacon-based discovery module

Figure 8.11: General functionality of the beacon-based discovery module. Channel policies are embedded by privacy-affecting entities in wirelessly broadcasted PriFi beacons.

devices or surveillance systems) to which the user and the privacy agent do and should not have access. In the running use case (see Section 5.5.1) the webcam and surveillance camera are examples of such systems. In shared environments (e.g., an office or the home of other persons when being there as a guest) privacy-affecting systems might also not be accessible by the user. For instance, the cleaning robot or automatic door opening system in the coming home use case (see Section 5.5.3) from the point of view of a guest.

As illustrated in Figure 8.11, the beacon-based discovery module assumes that such systems provide their channel policies in form of privacy beacons [389]. Privacy beacons are periodically and wirelessly broadcasted in the physical proximity of deployed systems or in proximity of the affected area in which privacy implications occur. The beacon-based discovery module receives those beacons, extracts contained channel policies and forwards them to the privacy engine. We call such beacons PriFi beacons with respect to the underlying WiFi technology, which will be discussed in the following section. We have previously published parts of the following discussion in [6].

8.4.1 PriFi beacons

The main design goals for effective announcements of privacy implications in shared and public environments are minimal connection overhead, fast and reliable transmission, and scalability. Most existing wireless technologies require initial connection establishment to exchange data. A possible solution to mitigate a required connection is to utilize customizable information in discovery or setup processes.

Our proposed PriFi beacons utilize information elements of IEEE 802.11 beacons [315] (WiFi beacons) to piggyback channel policies and to broadcast them in a system’s proximity. WiFi beacons are typically used to announce available WiFi networks. The approach allows simple and fast discovery of privacy implications without the need of a preliminary established connection. Leveraging WiFi beacons has the further advantage that in many shared or public environments with privacy implications, WiFi access points are already deployed.
WiFi beacons provide two possible ways of integrating custom data in so-called information elements, see Figure 8.12. Information elements are appended to beacons in order to carry optional information. The first way is leveraging the service set identifier (SSID) information element, which is typically used for user-friendly names of WiFi access points. However, SSIDs are limited to only 32 bytes, which requires channel policies to be highly compressed. Thus, an alternative approach is to embed not the complete channel policy in the SSID but only a policy reference, e.g., in form of a URI which allows to fetch the policy subsequently (as also described in Section 7.3.1).

The second way to embed a channel policy in WiFi beacons is the use of vendor-specific information elements, which allow to carry nonstandard information. A single information element can carry up to 252 bytes of payload. An information element of the same type can be appended multiple times, which allows to transmit a maximum payload of 2,213 bytes in one beacon frame. Because a channel policy is typically smaller than 1 kilobyte (e.g., in xml format), it can be piggybacked on a single beacon frame. Larger channel policies could be split into multiple fragments contained in multiple beacons as proposed by Chandra et al. [143]. However, this approach decreases the reliability of transmissions. Thus, an alternative approach would be the use of a short-form encoding for larger channel policies.

Typically, each channel policy is broadcasted via a separate PriFi beacon. However, in case of a central UbiComp system with several sub-entities, it makes sense to combine policies into a single beacon to avoid unnecessary transmissions. Thus, all policies can be included (e.g., at offices or train stations). Thus, in many cases no additional infrastructure is required.

Figure 8.12: Frame format of WiFi beacons as defined in the IEEE 802.11 standard [315]. Channel policies and policy references can be embedded in the SSID and vendor-specific information elements.
in multiple vendor-specific information elements of the same beacon if not exceeding the maximum payload.

We propose PriFi beacons as a combination of SSID and vendor-specific information element customization. Although attaching custom information elements is standard compliant, existing WiFi drivers require manual patching in order to pass custom information elements to the application level. Thus, we also use customized SSIDs to provide a fallback mechanism for non-patched devices.

8.4.2 Implementation

We implemented a prototype of our beaconing approach that enables devices and systems to send PriFi beacons. The prototype is based on a Raspberry Pi that has been equipped with a USB-WiFi dongle (RT2870/RT3070 chipset). The WiFi dongle runs in monitor mode in order to send custom WiFi frames. We used the Python library Scapy [580] to frame the PriFi beacons and transmit them with a beacon interval of 500ms.

A webcam (Logitech Webcam Pro 9000) and cleaning robot (iRobot Roomba 581) have been equipped with such Pis in order to broadcast observation and disturbances related channel policies, see Figure 8.13. The policies corresponded to the coming home use case (Section 5.5.3), thus the video camera forwards the observation channel to the smart home system and the cleaning robot will start its cleaning process in 5 minutes. Both policies also provided control points to users in the same WPA-protected WiFi network. Thus, while the beaconing approach supports privacy awareness for all users in proximity, it can also support privacy control for privileged users, i.e., only to those users that have valid credentials to access the network. In the coming home use case, this could be used to provide awareness of disturbances stemming from the cleaning robot and awareness of observations stemming from the video camera and the door system for guests, and at the same time provide control for home owners (i.e., Alice and Bob).
Currently, the range of PriFi beacons can only be adapted by changing the sender’s signal strength. Using directed antennas or other related geo-fencing techniques [345, 590] could allow to broadcast PriFi beacons in affected areas only (e.g., for the web cam and surveillance camera in the running use case). Another approach is to embed the affected area in the channel policies. For cameras we propose to embed the area either defined as absolute coordinates, or defined relatively via the camera’s position, height, angle of view, and the two directions limiting the camera’s field of view as illustrated in Figure 8.14.

On the user side, the beacon-based discovery module was implemented as part of a user’s privacy agent on an Android based smartphone. To support the extraction of channel policies from the customized information elements we needed to patch the Android WiFi stack (version 4.0.4). Changes were required in the underlying wpa supplicant [428] and the Android application framework in order to pass channel policies to the discovery module, which has been implemented as an Android service.

In order to visualize captured channel policies we implemented a preliminary privacy awareness application, which allows to view privacy-affecting entities and supports the access of control point references, see Figure 8.15. For the privileged home owners this allows control of the PriFi-enabled video camera and PriFi enabled cleaning robot via web-based control points. To also enable users with unpatched devices to discover privacy implications, the PriFi beacon’s SSID contained policy references and was composed of the string PB|<URL>, where PB stands for PriFi beacon and <URL> refers to a remote location of the entity’s channel policy, which was subsequently fetched by the application.

**Performance**

On most Android devices, the default scan interval for new WiFi networks (i.e., by collecting WiFi beacons) is set to 15 seconds. Due to power saving purposes we have not modified this interval, which also limits the update frequency of changed privacy implications to this time frame. However, for most scenarios this delay is acceptable as privacy implications are typically not frequently changing (e.g.,
implications of a surveillance system). An alternative technology for policy broadcasting is Bluetooth low energy [103], which supports the transmission of Bluetooth beacons (advertising packets) with lower power consumption. The drawback of the technology is the limited range of up to 10 meters and the maximum payload of only 31 bytes, which would only allow to embed policy references. Further, at the time of the prototype integration, Bluetooth low energy was not fully supported yet in the Android developer framework.

8.4.3 Discussion

The beacon-based discovery module allows the seamless discovery of channel policies through wireless broadcasts. The approach is suited for all environments in which users have no direct access to the infrastructure of existing UbiComp systems. For instance, in the coming home use case, the beaconing approach would allow guests in front of the door to gain awareness about the fact that the automatic door opening system forwards a guest’s presence to the home owners. In the running use case the web cam and surveillance cameras could use the beaconing approach to make passersby aware of the ongoing video observations.
Our lightweight implementation on a Raspberry Pi showed that UbiComp systems could be easily extended with the beaconing approach in order to announce their channel policies in physical proximity. The client side implementation of the beacon-based discovery module further showed the feasibility of receiving PriFi beacons on an Android smartphone. However, as the successful reception of customized information elements requires a patched WiFi stack, we propose to add a fallback method with embedded policy references in a beacon’s SSID in order cope for compatibility issues.

8.4.4 Related work

Announcing privacy information in broadcast beacons has originally been proposed by Langheinrich [391] as part of his privacy awareness system pawS, see also Section 3.5.3. His prototype was based on infrared beacons, which require the receiver to be in visible range. Furthermore, the original privacy beacons contained extended P3P policies which did not consider potential disturbances as proposed as part of our channel policies.

Maganis et al. [424] propose the Sensor Tricoder, which allows users to receive privacy policies associated with environmental sensors and connected applications by scanning QR codes with their smartphones. QR codes are dynamically generated and shown on digital displays in order to provide up-to-date policies reflecting the current sensor status and its use by applications. The drawback of this approach is that users actively have to collect privacy policies and cannot be supported automatically in gaining privacy awareness.

From a technical point of view, the approach of using WiFi beacons to piggyback additional information has also been leveraged for proximity based social interactions [640, 142] or for delivering location-based advertisements [143]. As far as we are aware, we are the first to combine the privacy beacons concept with WiFi piggybacking.

8.5 Community-based discovery module

Similar to the beacon-based discovery module, the community-based discovery module aims at receiving channel policies in shared and public environments without requiring access to existing infrastructures. It further allows to collaboratively create channel policies for entities that do not provide policies on their own and therefore constitutes a pessimistic discovery approach. Figure 8.16 depicts the module’s general functionality. Policies are fetched from a central database as already discussed for the personal device module in Section 8.2. For policy requests the database acts as a conventional location-based service. That is, a request contains the user’s current location and a response contains channel policies related to privacy implications as-
8.5 Community-based Discovery Module

Figure 8.16: General functionality of the community-based discovery module. Users can add and modify observed privacy implications at a given location, which are uploaded to a central policy database. The database allows to fetch channel policies based on the user’s current location.

associated with this location. While such a location-based service can pose privacy risks on its own, e.g., by its ability to track users, it is assumed to be a trusted service which provides a valid channel policy for respective observation channels. This could be achieved by developing such a service as an open-source project and deploying the database on a trusted infrastructure of existing nonprofit privacy organizations, e.g., Privacy International [523] or the Electronic Privacy Information Center [216].

The database can be collaboratively updated in a crowd-sourced fashion, either by users or system operators. For instance, users can add or modify information about public video cameras (e.g., public webcams or surveillance cameras). Such information could involve the position of a camera, its type (e.g., bullet or dome cameras), the mounted height, or the field of view. For some cameras users might even know the purpose of its operation, e.g., traffic guidance or security. However, detailed information about how a camera is operated and how its video stream is handled can only be provided by the operator of a camera. Thus, we assume that operators also have access to the database in order to complete missing or false information.

An underlying requirement for user-provided information on privacy implications of UbiComp systems is their observability. While video cameras often can be visually perceived, other devices and sensors might be invisibly embedded in the environment. The presence and privacy implications of such entities might only be implicitly inferred or guessed in some situations by a system’s behavior. For instance, privacy implications of a WiFi- and RFID-based location tracking system in a shopping mall for personalized advertisement. Further sources for gaining information about such implications might be signs on walls or privacy policy statements on websites. Other examples for privacy implications that can be collected by this crowd-sourced approach are environmental disturbances that follow a fixed
schedule. For instance, regular acoustic disturbances stemming from roadwork, public transport or street cleaning vehicles.

From the joint information of different parties, respective channel policies can be created and stored in the policy database. The crowd-sourced approach obviously only allows the collection of general privacy policies that are not associated with an individual user. Thus, this approach is best suited for public systems with static privacy implications. A good example of such systems today are public video cameras. Therefore, we focus our following discussion to the discovery of such cameras.

8.5.1 Discovery of public video cameras

We realized the community-based discovery module as a smartphone application with focus on supporting the crowd-sourced collection of information about public video cameras. In order to support the creation of detailed channel policies this information involves:

- **location**: The location of the camera should be provided by explicit coordinates.
- **affected area**: As mentioned in Section 8.4.2, the affected area can be defined as a set of coordinates or relatively via height, angle of view, and two directions for the camera’s field of view (see Figure 8.14).
- **operator**: This should refer to the entity (e.g., person or organization) who is responsible for the camera’s operation.
- **accessibility**: It should be specified who has access to the video stream and video recordings. This can either be specified generic as private or public, or by explicitly referencing entities. In the latter case operators should provide references to channel policies of respective entities. For public accessible cameras (e.g., webcams) these should also contain the references to the video stream (e.g., the URL of the camera’s website).
- **purpose**: The purpose of a camera’s operation, e.g., security, traffic, or webcam.
- **features**: A camera’s features should provide information about further privacy-affecting properties, such as adjustable zoom and rotation, night vision, or infrared vision.
- **retention**: Operators should specify whether a video stream is stored. For stored video recordings they should further specify the retention period.

---

6 While the conceptual work has been conducted by the author, the application was developed as part of the bachelor thesis of Ewgenij Leibmann [401].
Figure 8.17: Screenshots of the crowd-sourced video privacy (CSVP) app, showing the main menu (left), the map view to add new cameras (middle), and the dialog to add additional camera information (right).

- **protection**: Security and privacy mechanisms which are applied to the video stream or captured video recordings should be provided by the operator. Only in rare cases this information can be given by users, e.g., for public webcams.

While most information can be collected by users, some information can only reliably be provided by a camera’s operator. In particular the retention, protection, and accessibility of a camera are required to be provided by the operator.

In addition to supporting users in the collection of this information, the smartphone application should also make users aware of privacy implications of surrounding video cameras. Awareness can be gained either by explicitly viewing a map of surrounding cameras at the users current position or by viewing a history map that shows cameras in which’s field of view the user has been in the past. Users can further configure to be notified when entering a camera’s field of view, either for all cameras or only for cameras filtered by one or more of the information factors described above. This could enable a privacy-friendly walk navigation, for instance.

**Implementation**

We implemented an Android-based prototype of our crowd-sourced video privacy (CSVP) app leveraging Google’s maps API. The prototype allows to add new cameras via placing landmarks on a map view and subsequently enter additional information, see Figure 8.17. Adding the direction and angle of a camera is automatically supported by leveraging the smartphone’s gyroscope and magnetometer while directing the smartphone towards the camera’s lens. Users can
further browse a map of surrounding cameras and request detailed information about each camera by selecting its icon (see Figure 8.18).

The application is connected to a central webserver, which stores user provided camera information in a PostgreSQL database (v8.4) and supports location based queries of camera entries through the PostGIS extension (v2.1.3). For a future version of the application we plan to add camera information to the OpenStreetMap (OSM) database. The OSM community previously proposed some map keys for tagging video cameras which are similar to our proposed camera information listed above.

8.5.2 Evaluation

We evaluated the utility of our prototype in a preliminary field study with 12 participants located in the city center of Ulm. Participants had to walk a predefined path in the field of view of 4 different cameras, see Figure 8.19. The distance between two subsequent cameras was always less than 100 meters and the complete path could be walked in less than 5 minutes. The 4 cameras are depicted in Figure 8.20. The first camera a) is a wall-mounted outdoor surveillance camera directed towards book shelves standing in front of a book store. The second camera b) is a ceiling mounted dome camera for indoor surveillance of a bank’s entry area. Camera c) is a public webcam that is deployed behind a window in the top of a building and is directed to a large public square in front of the Ulm Minster. The camera can be accessed online where users are able to see the live stream and can further control zoom and rotation of the camera. The last camera on the path d) is a ceiling mounted dome camera for surveillance of a shop’s entry area.
Participants were asked to walk the path and to identify all existing video cameras in which’s field of view one might be along the path. We divided participants into two groups of 6 persons each. The control group was not equipped with our prototype application and thus was required to search visible installed cameras. The second group was supported in finding cameras with our prototype.

After finishing the path, all 12 participants were introduced in using the application for registering new cameras and subsequently had to add information for all 4 cameras while walking the path back in reverse order. Finally, participants filled out a brief usability questionnaire. In average each run took 13 minutes per participant. As a reward participants received ice cream after the study.

All participants were students of different fields with an age between 20 and 30 (20-25:7; 25-30:5). Gender was equally distributed in both groups.
Results: awareness

Figure 8.21 shows the number of persons for each group who realized on their own that they were in a video camera’s field of view. As expected, participants supported by the prototype identified more cameras than participants of the control group.

In total only three participants stated to be in the field of view of camera a). However, while for the control group this was due to the fact that most participants (5) were not aware of the camera, all participants supported by the prototype did notice the camera. But only two of them found themselves being in its field of view. Because the path was close to the camera but not directly in its field of view, it was hard to decide for participants in this situation. Also the second camera b) was noticed by all participants supported by the prototype, but one participant stated not being in its field of view as it was an indoor camera. However, the direction of the camera also captures people passing by. While also three participants of the control group recognized the camera, this was likely because surveillance cameras are expected in the area of a bank. The most obvious difference was found for the public webcam c). All participants supported by the prototype did notice to be in its field of view even though they could not see the camera. Most participants tried to find the camera while standing in its field of view. Only one participant of the control group stated to be in the field of view of camera c) because he knew the website and was aware of this camera before. The final camera was identified by almost all participants from both groups because the path ended in the entry area of the shop next to the camera. Only one participant of the control group stated not being in its field of view as he expected the camera to be directed to a different side.

After finishing the path, participants from both groups were asked to rate the importance of additional information about a video camera. The results are depicted in Figure 8.22. Most important for participants was a camera’s location, the affected area, and information about its accessibility, followed by the operator, height, and purpose.
of its operation. While most participants (8) found the applied protection mechanisms very important, two participants considered this information as not very important. The type of the camera as well as the camera’s mounting (e.g., wall or ceiling) was considered as the least important information.

Asking participants in which situations they would likely use the app, 5 stated “unknown cities”, 2 stated “public places”, and one stated in situations when carrying a lot of money. One female participant also stated to likely use the app for safety purposes in order to find a path with many surveillance cameras when going home alone at night. This shows that the utility of the application is not limited to privacy purposes.

Results: registration usability

The usability of our prototype is confirmed by the results of the ASQ [404] questionnaire shown in Figure 8.23, which highlights that participants were satisfied with the required time and effort for registering a camera. While participants found most of the requested camera information comprehensible, some participants had trouble to understand the protection (3) and the accessibility (5) information. This might be caused by the fact that this information typically should be provided by a camera’s operator and can only be guessed by users.
Results: registration accuracy

The accuracy of the entered location of each camera and the variation of its entered orientation, angle, and height are depicted in Figure 8.24. The entered location of cameras a), b), and d) was quite accurate for all participants as shown by the low variance of the red clusters. The higher variance in entered locations of the public webcam c) was due to the fact, that participants could not see the camera and thus did not know the exact location.

The mounted height of each camera was guessed by participants. The height of camera a) and d) was consistently guessed as 2 meters. Also the guessed height of camera b) only showed a low variance. Again camera c) shows the highest variance in its guessed height due to its hidden nature. A possible approach to address such deviations is to calculate the values by combining the reported information of multiple users.

The orientation and angle of each camera was automatically measured when participants were holding the smartphone towards a camera’s lens in the center of its assumed field of view. While the variance of most entries is acceptable, we can see a higher variance of the orientation of camera b) and of the angle of camera a). The high variance of camera b)’s orientation was caused by the dome type of the camera, which makes it difficult to see its real orientation. While camera d) was also a dome camera, participants were standing directly next to this camera and could see its orientation. When registering camera b) participants were standing in a distance of more than 10 meters. The
variance in the angle of camera a) was caused by the fact that participants walked over to the camera and were standing in different distance when targeting its lens. While this was also true for camera c), the distance to the camera was much higher and thus had a lower effect on the measured angle.

Participants also entered additional information about a camera’s operator, purpose, camera type, mounting, protection, and accessibility. While the operator, camera type, mounting, and protection were consistent among participants (protection was always unknown), a higher variance was observed for the other information. For the purpose, participants could choose from the predefined set (private, public, traffic, security), which was found to be confusing as private and public were perceived as accessibility categories rather than a purpose category. The set of possible accessibility categories was unknown, private, public, business, and government. Here participants had no consistent conception of private and business as the shop/bank cameras a), b), and d) were tagged with both categories. This highlights that a common understanding of different camera information is required and needs further investigation.

8.5.3 Discussion

The goal of the community-based discovery module is the support of privacy awareness in situations in which privacy implications cannot be discovered by one of the other discovery modules. Examples are public video cameras that do not support our proposed beaconing approach discussed in Section 8.4.1. Therefore, we realized a crowd-sourced video privacy application as a first step to realize the community-based discovery module.

The results of the first part of our field trial show that the prototype effectively makes users aware of surrounding cameras. While in areas where cameras are expected (e.g., in shops or banks) the application might not be required to make persons aware it nevertheless could be used to gain additional information about existing cameras (e.g., their purpose or accessibility), which all participants valued as an important feature. The advantage of our prototype is especially emerging in situations with hidden, unexpected, or unknown cameras such as the public webcam in our field trial. This is also aligned to the reported places where participants would likely use the app: in unknown cities and public places.

The results of the second study part show that a crowd-sourced approach of registering video cameras is feasible and that the prototype effectively can support users in the registration process. However, users need further guidance in providing additional camera information in order to obtain a consistent database. A possible solution to mitigate this issue would be that a single camera entry is
calculated by the entered information of multiple users or entries are approved among users. False or incomplete information should also be rectifiable by the camera’s operator.

Our prototype confirmed the feasibility of the community-based discovery approach and showed its potential in collecting information about privacy implications. In order to facilitate the integration of our implementation into the privacy agent, the next step would be to convert the collected information into actual channel policies. This can either be implemented on the client side in the discovery module or in the database of the community as proposed before.

8.5.4 Related work

Collaborative community based or crowd-sourced approaches for enhancing privacy have been previously proposed for websites [292, 365, 121, 62], emails [335], or mobile applications [409, 648]. However, most of these approaches primarily focus on the collaborative identification of privacy policy violations or the generation of common privacy preferences.

Winkler and Rinner [693] proposed to combine the community based registration of video cameras with their concept of smart cameras that allow the attestation of additional meta information (see also Section 3.5.2). While their work focuses on the technical details of the attestation process, the registration of new cameras is not discussed.

The Spybuster community [355] was a first proposal that allowed the collaborative tagging of surveillance cameras with a mobile application. However, the prototype only allowed to enter a limited set of information and the hardware limitations of the mobile device only allowed for a radar-based visualization of cameras. A more detailed map view could be browsed on a website.

There have been also investigations to add surveillance camera information to the free OpenStreetMap database [492]. Already registered cameras can be found on a website [496] with a similar visualization as used in our prototype. The proposed meta information for cameras are similar to those provided by our application, which makes the integration into OSM a valuable extension for future work.

8.6 Privacy Signaling Module

The feasibility of enforcing privacy preferences as discussed in the previous sections primarily depends on the assumption that systems provide control points. However, in some situations a system might not be willing to share these control points and only allows implicit control by receiving a user’s privacy preferences. Direct control might further be limited or inapplicable in multi-user situations due to differing control intentions among users. While not only systems but
also other persons can affect one’s privacy, other persons obviously
cannot be controlled directly either. In all such situations indirect con-
trol can be applied through the signaling of privacy preferences to
other entities.

In order to achieve this, the privacy engine forwards a user’s pre-
configured privacy preferences to the privacy signaling module, which
wirelessly broadcasts these preferences in the user’s physical proxim-
ity (see Figure 8.25). Similar to channel policies, the preferences are
embedded in wireless privacy preference (PriPref) beacons, which are
received by environmental systems or persons.

We envision this signaling approach to be particularly effective in
situations with potential disturbances stemming from surrounding
systems or persons in shared and public environments (e.g., offices or
public transport). An example is the working use case with a shared
office, see Section 5.5.2. Several studies [118, 181, 99, 193] have shown
that disturbances in open-plan offices reduce employees’ satisfaction
and perceptions of privacy, especially in terms of visual and acous-
tical privacy [193]. See also Section 4.1 for a discussion of general
disturbances.

Typical sources of undesired disturbances in shared and public en-
vironments are loud conversations [212], phone calls [461, 238], or an-
noying ringtones [320]. In such situations, it is usually inconvenient
or awkward to signal personal privacy preferences to such disturbers.
For instance, if one would prefer quietness to work or sleep and oth-
ers are being noisy, one must directly approach the disturbers, which
may cause socially awkward or unpleasant situations.

The privacy signaling module allows broadcasting user-defined pri-
vacy preferences (PriPref) in one’s physical proximity as an approach
to express privacy preferences in an anonymous way without requiring
to confront the respective disturber. This way, surrounding per-
sons can learn about the privacy preferences of other present per-
sons and adopt their behavior accordingly. Furthermore, devices and
systems receiving such preferences can automatically adapt to the dominant preferences of all persons in the current environment. For instance, smartphones could switch to “vibrate only” if the majority of present persons signals a need for quiet.

In the next section we will first discuss the results of an online survey with 101 participants that we conducted to elicit common sources of everyday disturbances and in which situations they occur. From the results, we derived the most relevant disturbances participants wanted to reduce in everyday situations, e.g., at work or on public transport. These disturbances determined the types of privacy preferences supported by our prototype implementation in form of a mobile application.\(^7\) The prototype allows users to create profiles for different situations, broadcast their preferences when desired, and learn about the privacy preferences of other present persons. It further supports the automatic adaptation of phone settings according to the dominant preferences in the current environment. We evaluated our prototype in preliminary usability experiments (n=10) and a five-day field trial with 28 participants. We previously discussed parts of the following sections in \([7]\).

### 8.6.1 Disturbances in everyday life

In order to determine what privacy preferences would be relevant to consider and should be supported by the signaling module, we conducted an online survey to gain insights on common disturbances in everyday life, and how individuals deal with them. Furthermore, we asked participants to rate the perceived utility of a smartphone application that would allow them to anonymously share their privacy preferences with others nearby, whether they would be interested in knowing about others’ preferences, and the perceived utility of their phone automatically adapting to those preferences.

**Participants**

Participants were primarily recruited from our campus population, which corresponds to a relevant target group for our prototype application. The survey was completed by 101 participants between 18 and 57 years old (M=23), with 65 male and 36 female. Participants were well educated (61% high school degree, 33% university degree) and almost all owned a smartphone (95%). Furthermore, most participants (98%) were German. Thus, our results may primarily reflect norms of German culture, with potential deviations in other demographics.

---

\(^7\) The application has been developed as part of the bachelor thesis of Sebastian Thoma \([645]\).
Results: common disturbances

Figure 8.26 shows the reported frequencies of common disturbances, where they occur, and what activities they impact. For each item we ran a Mann-Whitney U test to evaluate gender-specific differences. While no significant differences could be found for the source of disturbances and the impacted activities, we found significant differences for some of the reported locations.
The majority of participants (87.5%) reported feeling frequently or sometimes disturbed by loud music, followed by others’ phone calls (71.9%), ringing phones (66.7%) and nearby conversations (61.5%). The more distracting nature of phone calls in relation to face-to-face conversations has also been confirmed by previous research [212, 238]. Reasons for that are the missing pieces of a conversation which one tries to complete and the fact that people tend to speak louder in phone calls than in normal conversations [238]. Less common disturbances were noise of devices, and being photographed or approached by others. Further disturbances mentioned by individual participants were loud typing, notifications during a date, and crying babies.

Regarding reported locations, disturbances occur primarily during public transport (79.2%) and at university (67%), which reflects characteristics of the sample population. Almost half of the participants also stated to be frequently or sometimes disturbed in restaurants, at work, public places, and in supermarkets or shops. Disturbances occurred less often at home or at the library. Further individually mentioned locations of frequent disturbances were train stations, waiting rooms, cinemas, and fitness studios. We found significant gender-specific differences for four locations. Women reported to be more frequently disturbed at restaurants (U = 3612, p = .005), at libraries (U = 3719, p = .011), in supermarkets/shops (U = 3737, p = .013), and during public transport (U = 3785, p = .019).

The most named disturbed activities were studying (75%), working (57.3%), and reading (54.2%). Individual participants mentioned dating, cooking, and cleaning as frequently disturbed activities.

Based on these results we derived salient disturbance factors that allow users to specify privacy preferences for different situations. These factors will be discussed in the next section 8.6.2.

Results: reducing disturbances

We further asked participants about their strategies for reducing physical disturbances, and about their attitude towards a smartphone application that would support them in such situations. The results are shown in Figure 8.27.

Roughly half of the participants stated to frequently or sometimes take counter-measures to reduce disturbances. However, only 27% stated to actively approach others who cause disturbances. Most participants (73%) rarely or never confronted disturbers as it makes them feel uncomfortable (68%). Of the 60 participants who stated to approach other persons, only 28% reported that it often led to the end of the disturbance. Most (63%) were only successful in stopping the disturbance in some situations and 8% reported to never succeeding in this regard. We further found a significant gender-specific difference in the reported frequency of approaching others and the success of approaching. Men approach disturbers more frequently (U = 1373,
Figure 8.27: Frequency of counter-measures to reduce disturbances together with success and feeling when approaching others (top). Attitudes towards app features for supporting the reduction of disturbances (bottom).

\( p=0.05 \) and also reported succeeding more often in stopping a disturbance by approaching its source (\( U=549, \ p=0.025 \)).

The reported experienced reactions of the persons approached varied from considerate or ashamed, to annoyed and violent. Negative reactions were primarily encountered in public transport. Therefore, instead of approaching disturbers, some participants reported to prefer changing their location if possible (5) (e.g., to a different seat on the train) or to isolate themselves from disturbances (6) (e.g., by listening to music with their headphones).

Regarding the support of reducing disturbances by a smartphone app, most participants (84%) would use it for the automatic adaptation of phone settings in order to reduce disturbances, but primarily based on own preferences. Only 39% would allow automatic adaptation based on preferences received from persons nearby. On the other side, roughly half of the participants could imagine to use such an app to share their own privacy preferences (54%) and having devices...
of other persons adapt to their communicated preferences (52%). This shows that the acceptance for using the app for reducing disturbances by others is higher than for reducing one’s own disturbance of others. However, 38% could imagine informing themselves about others’ preferences – mostly in public places like public transport, restaurants, and waiting rooms. 58% of the participants also stated they would change their behavior in some situations, if such an application would inform them about others’ preferences. Here we found that men were significantly more likely to potentially change their behavior than women (U=1384, p=0.028).

8.6.2 Signaling privacy preferences

Based on the survey results, we defined a set of privacy preference dimensions and developed wireless broadcasting mechanisms to enable users to signal their privacy preferences in their physical proximity.

Salient disturbance factors

From the survey results and the common sources of everyday disturbances in particular (see Figure 8.26), we derived six salient disturbance factors for which users can specify their preferences:

1. **Loudness**: Users can specify how accepting they are of loud noise or sounds nearby, or whether they prefer quiet. This factor concerns the general sound level in a user’s environment. This includes loud music, which was the most frequently reported source of disturbance in our online survey.

2. **Disturbances**: Users can specify their acceptance of specific acoustic disturbances, e.g., ringing phones or noise from typing.

3. **Conversations**: Whether users approve of conversations between nearby persons and of phone calls taking place in their vicinity.

4. **Contacting**: Whether users are open to being approached by others. While being approached was a less frequent source of disturbance in our survey, we chose to include this factor in order to study its utility in real world situations.

5. **Pictures**: Whether users mind it when they are in other people’s photos or when others take pictures of them. This factor concerns pictures being taken while the user is in the camera’s field of view, regardless of whether this is intended or unintended by the person taking the picture.

6. **Videos**: This factor is the same as the pictures factor but pertains to video recording, either by other persons or surveillance cameras. We included this dimension, because video recording can be considered more invasive than taking single pictures and hence should be reflected as a separate factor.
The user’s level of acceptance of a given disturbance factor can be specified on a 3-point acceptance scale: accept, tolerate, and reject (see Figure 8.28). Accepting a factor means that the user is open to it in the current situation, i.e., it is not perceived as a disturbance. For example, accepting loudness means that the user does currently not mind loud music or a loud environment. Tolerating a factor means that the user would currently prefer a reduction of the disturbance but also accepts it. Finally, if a factor is rejected the user has a strong preference against this factor. For example, a user might reject loudness during activities that require quiet, such as studying or working, which were the two most frequently reported disturbed activities.

To ease preference management, our signaling application enables users to specify preference profiles for recurring situations. For example, a user may create profiles related to activities such as studying, working, relaxing, or reading.

Preference broadcasting

In order to effectively signal a user’s privacy preferences to other persons nearby, we identified three basic requirements that must be met by potential broadcasting mechanisms:

- **Ad-hoc communication**: To allow fast and seamless communication of privacy preferences, a broadcasting mechanism should not rely on centralized solutions requiring Internet connectivity. Furthermore, ad-hoc communication should work without requiring lengthy connection establishment between devices.

- **Proximity-based communication**: Privacy preferences only need to be signaled to other persons nearby (potential disturbers). In order to provide a meaningful overview (see Figure 8.28) of the dominant privacy preferences in a receiver’s current environment, broadcasting of privacy preferences should be limited to the range required for reaching those potential disturbers.
• **Existing technology:** Signaling mechanisms should be based on existing and widely available technology to facilitate fast adoption and increase the utility of signaling privacy preferences. Requiring special technology would unnecessarily limit the number of potential receivers of broadcast preferences.

Based on these requirements, we developed two independent wireless broadcast mechanisms that leverage WiFi and Bluetooth, respectively. Both technologies are available on most smartphones and mobile devices and have a range of 10–100 meters, which covers the physical area around a user in which potential disturbers may be located. While both technologies typically require the establishment of a connection, we avoid connection establishment by embedding privacy preferences directly into WiFi beacon messages and Bluetooth device names, which can be received by other devices without the need of a connection.

Supporting signaling over two technologies further has the advantage that our system can dynamically switch between them depending on which one is currently not in use for other purposes on a user’s mobile device, e.g., using WiFi for preference signaling when Bluetooth is used for a headset connection. The approach of embedding custom information in WiFi beacons has been already discussed for PriPref beacons in Section 8.4.1. These beacons can be used to communicate custom information by either encoding it in the service set identifier (SSID) or optional information elements.

Similar to the SSID method, Bluetooth device names can also be leveraged to broadcast custom information of up to 248 bytes. Davies et al. [179] used this approach to advertise public display interaction. The Bluetooth discovery process is more energy efficient than scanning for WiFi beacons, but takes significantly longer. Therefore, we propose to combine both methods and to primarily use WiFi unless the battery level is low or the device is currently using the WiFi connection to transmit or receive data.

We encode privacy preferences in a plain text string that starts with the prefix `pripref`, followed by the 6 disturbance factors in the order given in the previous section. For each disturbance factor, the user’s acceptance is coded by a single digit: 1 (accept), 2 (tolerate), or 3 (reject). For example, the string `pripref:323123` encodes the preference: reject loudness, tolerate disturbances, reject conversations, accept contacting, tolerate pictures, and reject videos. Note that this encoding scheme is extensible. Further acceptance levels as well as disturbance factors could be added in the future.

Our current prototype implementation does not yet include integrity protection mechanisms to protect against forged preference broadcasts. The anonymity of broadcasts further depends on the assumption that the Bluetooth or WiFi MAC address cannot be associated with a particular person. Both issues can likely be addressed...
by leveraging pseudonyms and digital signatures similar to proposals for ad-hoc car-to-car communications [515]. The concept of anonymous credentials [130, 82] could be used to further enhance the unlinkability between a user and her individual privacy preferences.

8.6.3 Dynamic settings adaptation

When privacy preferences are signaled with either approach outlined above, the preferences are received by devices of other persons in range and processed by our application. Accumulated received preferences can provide an overview of the prevalent preferences in the current environment. However, based on others’ received preferences, our system can also automatically adapt device settings, such as the volume, vibration mode, and call forwarding settings. Whether adaptation is required is determined based on the first three disturbance factors, loudness, disturbances, and conversations. The other three disturbance factors are typically not influenced by the settings of a mobile device. However, if device settings would allow to block the camera and video function, this could pose another possible adaptation. We currently support three possible adaptation decisions, to demonstrate the potential of dynamic settings adaptation:

1. **Reduce volume and system sound**: This is applied when the majority of persons in proximity prefers a quiet environment, that is more than 50% reject loudness.

2. **Mute and activate vibration mode**: This is applied when the majority (>50%) rejects acoustic disturbances.

3. **Redirect incoming calls to mailbox**: This is applied when conversations are rejected by the majority (>50%).

While adaptation decision 3 is independent of the other two decisions, decision 2 obviously outweighs decision 1. Thus, regarding acoustic noise of a mobile device the disturbance factor is weighted higher as the loudness factor, in our current adaptation mechanism. Further, tolerated factors are not respected in the adaptation mechanism but could support more nuanced adaptations in a future version. All three adaptations can be manually enabled or disabled.

**Mobile application**

We implemented the features described above in *PriPref Broadcaster*, which is a mobile application for Android. We created two versions of our system. Our fully functional prototype is based on a custom Android image in which we patched the WiFi device drivers in order to enable broadcasting and receiving WiFi beacons with information
elements. We further created a public version\footnote{PriPref Broadcaster is available in the Google Play store: \url{https://play.google.com/store/apps/details?id=com.pripref.app}} that only uses Bluetooth to broadcast preferences and, hence, can be readily installed and used on any unpatched Android phone.

Figure 8.28 gives an overview of the application. In the main view, users can set their preferences, create profiles, and start/stop the broadcasting of their preferences. The acceptance levels are represented with the traffic lights metaphor (green=accept, yellow=tolerate, red=reject). The second view provides an overview about the preferences of other persons present in the user’s proximity. While the first version of the app used a pie chart visualization for this overview the usability study revealed that this approach was counter-intuitive. Thus, the final version (shown in Figure 8.28) uses a visualization similar to the settings view. To ensure that minorities with more restrictive preferences are properly visible, red is displayed when at least some persons reject a factor, and if persons rejecting and tolerating this factor exceed 50% together. In all other cases the acceptance factor is averaged across all received broadcasts. Three symbols at the bottom of the view further show if and how the settings of the user’s phone have been automatically adapted based on those received preferences, i.e., if the phone’s volume has been changed, the vibration settings have been changed, or call forwarding has been activated. Finally, the adaptation settings view enables users to control whether phone settings should be automatically adapted at all, and to enable/disable automatic adaptation of volume, vibrations, and call forwarding.

8.6.4 Usability study

We first conducted a usability study with an initial prototype version. The results informed the design of the public version of our app, shown in Figure 8.28. The usability study was conducted with 10 computer science students (2 female, 8 male; avg. age 25 years, SD=3). After a short introduction to the app, participants performed seven tasks that covered all app features: profile creation (t1), changing (t2) and deletion (t3); broadcast starting (t4) and stopping (t5); adaptation configuration (t6); and gaining an overview of others’ preferences (t7). Participants completed the ASQ questionnaire \cite{404} after each task, and the PSSUQ \cite{404} at the end, followed by a short interview.

Results

Figure 8.29 shows the positive feedback of participants for ASQ and PSSUQ, respectively. All tasks were rated as satisfactory (above neutral) in the ASQ. Only the configuration of adaptation (t6) and inform-
ing about others’ preferences (t7) received slightly lower scores. The interviews revealed that adaptation configuration was rated lower, because the menu for opening the adaptation view was not available from all views. Information about others’ preferences was rated lower due to a counter-intuitive pie chart visualization of others’ preferences. Both issues have been addressed in the design of the public version of our application, shown in Figure 8.28.

The exit interviews further revealed that all of the ten participants saw utility in our application and found it easy to use. Nine participants stated that they could imagine using the app in everyday situations and remarked on several situations in the past (e.g., at work or in public transport), in which the app would have been useful.

8.6.5 Field trial

To investigate how PriPref Broadcaster would be used in everyday situations, we conducted a 5-day field trial with a deployment on devices of 28 participants, who were students and employees recruited from our campus population.

Participants were asked to adjust the app settings during their daily activities, whenever their actual privacy preferences changed. They were further asked to create profiles for recurring situations, if they thought it would be useful, and to start broadcasting when they wanted others to know about their preferences. Furthermore, they should configure adaptation settings as preferred. The app automatically reminded them to provide feedback on their usage every 5 hours. After using the app for 5 days, participants were asked to answer a post study questionnaire and to provide demographic data. In addition, the application logged whenever broadcasting was started or stopped, adaptation settings changed, own preferences or received preferences of present persons changed, and when the user viewed others’ preferences. As a reward, participants could enter into a lottery of 5 shopping coupons with a value of 10 to 50 Euros.
Participants

Participants consisted of 2 groups. Most of them (24) freely installed the app motivated by distributed flyers on our university campus. Those participants took part in the study anonymously by downloading the app from Google Play and using it at their discretion. Because we could not assure that those participants were in physical proximity of each other when using the app, we were primarily interested in how they would use the app for specifying privacy preferences. Of those 24 participants, 13 provided demographic data (all male, 10 students and 3 employees) and 15 provided explicit usage feedback. Furthermore, 10 persons used the app for the complete duration of 5 days, while others used the app only for 3 days (2), 2 days (5), and one day (8). We did not collect contact information of participants to respect their anonymity and could therefore not probe why they did not use the app for the complete duration.

We further recruited a group of 4 students (3 male, 1 female), who regularly spent time together in a shared lab space at our institute, in which they worked or studied. This group allowed us to gain a better indication of the effectiveness of our approach when all persons in physical proximity are using the application. All participants of this group used the app for the complete duration of 5 days and provided explicit usage feedback.

Overall, the 17 persons who provided demographic data were aged between 18 and 31 (M=25) and most of them (16) had a computer science background.

Across all 28 participants who contributed data to our study, we logged 1,220 application events, of which 511 (x=18, M=4, SD=27) were environmental changes (i.e., the received preferences of nearby persons changed), 247 profile changes by the user (x=9, M=4, SD=11), 185 transmission starts to broadcast preferences (x=7, M=3, SD=11), 177 views of environmental preferences (x=5, M=3, SD=9), 83 transmission stops (x=3, M=3, SD=9), and 17 changes of adaptation settings (x=1, M=0, SD=1).

Results: situations of use

The explicit usage feedback provided by participants indicates that the app was mostly used while studying (34%), relaxing (28%), or working (22%), which corresponds to the results of our online survey. In the field study, participants used the app mainly at home (40%), at work/university (37%), and in public transport (11%). In the online survey, “at work” was indeed a frequently mentioned location where disturbances occur often, while “at home” was the least frequently named location, and “public transport” the most frequently mentioned location of disturbances. The low number of uses in public transport might be due to the low prevalence of the app and thus
lacking real effects of privacy preference broadcasts. In the post study survey one participant stated “I assumed that people do not have the app. So I wanted to save time and effort.” The large number of uses at home might be caused by the fact that participants described that they used the app in 39% of all cases for testing purposes, i.e., to play around with our app. In 43% it was used to reduce disturbances, and in 18% to avoid disturbing others. Thus, participants preferred to reduce disturbances caused by others by signaling privacy preferences, but were less interested in informing themselves of others’ preferences. While this reflects the results of our online survey (see Figure 8.27), the probing nature of the study, i.e., only few users have the app, made it unlikely for participants to receive preference broadcasts from other users in many situations, e.g., when not on campus.

In situations that prompted participants to change their privacy preferences, they categorized people around them as strangers in 42% of the cases, as friends in 31% as colleagues, as family members, and in 16% of all cases participants were alone when using the application. This result might support our assumption that the app is especially useful to communicate privacy preferences in situations with strangers, as directly approaching those people to mitigate disturbances may be unpleasant or socially awkward.

Results: preferences and profiles

In total, participants changed their preferences at 254 occasions. Figure 8.30 shows the distribution of configured preferences. While the first four disturbance factors (loudness, disturbances, conversations, and contacting) were considered acceptable in more than 50% of all preference configurations, picture taking (49.2%) and video recording (57.5%) were mostly rejected. Conversations (18.5%) and contacting (16.9%) received the lowest rejection rate compared to loudness (29.9%) and disturbances (33.1%). The results show that taking pictures and videos are major privacy concerns in most situations and that conversations and being approached are perceived as less disturbing than loudness and acoustic disturbances.

Participants created 76 preference profiles in total (avg=3.4; SD=2.1), from which we identified 7 profile categories: work (n=9), studying
(n=7), public transport (n=7), lunch break (n=6), leisure (n=5), home (n=5), and sleep/do not disturb (n=4). Figure 8.31 shows the average acceptance of the disturbance factors for each category. The most restrictive profile categories were sleep/don’t disturb, studying, and work.

Results: automatic adaptation

Four of the 28 participants enabled the automatic phone adaptation in 9 situations, mostly during studying and working (5). While volume adaptation was allowed in all cases, vibration adaptation was disabled once. Call forwarding was never allowed. The low acceptance of automatic adaptation was also confirmed in the post study survey. Only 3 participants stated they would use the mechanism in everyday situations. One participant stated that he would never use automatic call forwarding and another stated that he switched off adaptation as he was afraid that his alarm would be muted as well. However, all would use the app to signal their own preferences, and 80% indicated that they would use it to learn about others’ preferences.

Qualitative results

The four students who actively used the app in their shared work space independently reported liking the opportunity of sharing their preferences with the others. They stated that the app increased their awareness and consideration of each others’ preferences and in most situations reduced unwanted disturbances. However, in some situations they missed an option to more explicitly notify others about their preferences. One participant compensated the lack of explicit notifications by holding up his phone with the app displaying his preferences, which resulted in the end of a disturbance. Related to this, two participants stated that they would like to receive notifications whenever preferences of present persons changed in order to adapt their behavior accordingly.

Another participant further stated that he would like to be able to add more details about a disturbance or some short messages to the preferences in order to specify what aspects are specifically disturbing, e.g., what kind of conversations. One participant would have liked to be able to share preferences with his real identity rather than anonymously, at least in some situations. For instance, to allow others to know who does not want to be contacted.

Study limitations

A limitation of our evaluation is the sample size of 10 participants for the usability study and 28 participants for the field trial. As in the online survey, all participants were German, which might influence results due to cultural norms. Especially the preferences and common
### Figure 8.31: Common profiles created during the field trial and average acceptance of disturbance factors for each profile among participants.

<table>
<thead>
<tr>
<th>Profile Category</th>
<th>Loudness</th>
<th>Disturb.</th>
<th>Convers.</th>
<th>Contacting</th>
<th>Pictures</th>
<th>Videos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sleep /Don’t disturb</td>
<td>3.0 (SD=0)</td>
<td>2.8 (SD=0.5)</td>
<td>2.5 (SD=0.6)</td>
<td>2.5 (SD=0.6)</td>
<td>3.0 (SD=0)</td>
<td>3.0 (SD=0)</td>
</tr>
<tr>
<td>Studying</td>
<td>2.7 (SD=0.5)</td>
<td>2.5 (SD=0.8)</td>
<td>2.5 (SD=0.8)</td>
<td>1.7 (SD=0.8)</td>
<td>2.3 (SD=0.8)</td>
<td>2.5 (SD=0.8)</td>
</tr>
<tr>
<td>Work</td>
<td>2.2 (SD=0.7)</td>
<td>2.6 (SD=0.7)</td>
<td>2.0 (SD=0.9)</td>
<td>2.2 (SD=0.7)</td>
<td>2.6 (SD=0.7)</td>
<td>2.7 (SD=0.7)</td>
</tr>
<tr>
<td>Leisure</td>
<td>2.0 (SD=1.0)</td>
<td>2.0 (SD=0.7)</td>
<td>2.0 (SD=0.7)</td>
<td>2.2 (SD=1.1)</td>
<td>2.2 (SD=1.1)</td>
<td>2.2 (SD=1.1)</td>
</tr>
<tr>
<td>Home</td>
<td>1.6 (SD=0.9)</td>
<td>1.8 (SD=1.1)</td>
<td>1.8 (SD=1.1)</td>
<td>1.8 (SD=1.1)</td>
<td>2.2 (SD=1.1)</td>
<td>2.6 (SD=0.9)</td>
</tr>
<tr>
<td>Public Transport</td>
<td>1.3 (SD=0.5)</td>
<td>1.3 (SD=0.5)</td>
<td>1.3 (SD=0.8)</td>
<td>1.1 (SD=0.4)</td>
<td>2.5 (SD=0.5)</td>
<td>2.5 (SD=0.4)</td>
</tr>
<tr>
<td>Lunch Break</td>
<td>1.3 (SD=0.8)</td>
<td>1.3 (SD=0.8)</td>
<td>1.3 (SD=0.8)</td>
<td>1.3 (SD=0.8)</td>
<td>2.8 (SD=0.4)</td>
<td>2.8 (SD=0.4)</td>
</tr>
</tbody>
</table>

1=accept, 2=tolerate, 3=reject

---

8.6.6 Discussion

The results of our online survey revealed common sources of everyday disturbances, such as loud music, others’ phone calls and conversations, or photo taking. Most participants felt uncomfortable approaching others causing such disturbances. Especially women reported to less often confront disturbers, and if they do have low success in ending the disturbance. Our prototype implementation provides an anonymous and user-friendly approach to signal one’s privacy preferences concerning undesired disturbances in such situations. It allows users to learn about others’ preferences and to automatically adapt phone settings based on dominating preferences in the current environment.

While the results of our evaluation studies are promising and indicate that the concept of privacy preference signaling was highly accepted, perceived as useful, and would be used in many everyday situations, the effectiveness has only been confirmed in a limited setting, and requires further evaluation with larger participant groups. A major factor that influences the effectiveness of our approach is the required prevalence among users. The motivation of sharing prefer-
ences depends on the assumption that others can be made aware of one’s preferences and change their behavior accordingly. While our results suggest that automatic adaptation of phone settings is less accepted, the online survey and field trial showed that people nevertheless are willing to inform themselves about others’ preferences and indicate that they would adjust their behavior if required.

Providing awareness of privacy preferences even without a large number of application deployments could be supported via proxy devices, e.g., through public displays, which could visualize the combined preferences of persons nearby. For example, displays at study rooms or train compartments, as illustrated in Figure 8.32, could summarize dominant preferences of present persons. Persons could then choose a seat on the train or in the study area that best matches their own preferences or adjust their behavior accordingly. While such displays would only be able to communicate preferences of persons using the application, it could also motivate others to obtain and use the application as well in order to also signal their preferences.

Further, as suggested by several participants, a valuable extension would be targeted just-in-time notifications about others’ privacy preferences when a user starts an activity that would be against those preferences, e.g., when placing a phone call or opening the smartphone’s camera app. Highlighting others’ preferences in such situations could nudge people to behave more considerately with respect to those preferences.

With respect to our use case, the signaling approach is especially suited for the working use case (see Section 5.5.2) in order to mitigate undesired phone calls or conversations in the shared office. Preferences could be visualized on the display of the collaboration system in order to provide the benefits as discussed above. The relevance and effectiveness of privacy signaling in such shared environments has been confirmed by the collaborative usage of our prototype in a shared lab space during the field trial.
8.6.7 Related work

Only a small number of existing proposals have considered how users can signal privacy preferences to others. However, there has been some work on managing phone-related interruptions. We discuss relevant related work in both domains. Further related work on minimizing disturbances has been already discussed in Section 3.5.2.

Privacy signaling

Signaling of information-centric privacy preferences has previously been proposed in the web context. The “do not track” HTTP header is intended to communicate advertising opt-out preferences to websites [443]. Privicons [377] are icons that a sender can include in emails to signal recipients how the email should be handled (e.g., “keep secret” or “don’t print”).

We combined the concept of privacy icons with cryptographic privacy enforcement in our own work on PrivacyJudge [8]. PrivacyJudge allows users to keep control of information published in online social networks and to signal own privacy preferences to other users in order to prevent undesired actions on personal information. We argue that in a social context privacy signaling should always complement enforcement mechanisms because privacy hardly can be enforced with full guarantee. For instance, once a user has access to a private picture on an online social network site he will always be able to make a screenshot or to manually take a picture of the screen with another device.

While the previous approaches allow to signal information privacy preferences online, hardly any work has considered how individuals can be supported in signaling their territorial privacy needs to surrounding UbiComp devices or to other persons. One example is the interactive door “Shoji” [394]. It uses colored areas and brightness levels on its surface to signal disturbance-related privacy preferences (e.g., “do not disturb”) to roommates in shared apartments. Roesner et al. [543] propose world-driven access control to signal privacy preferences to environmental sensors, e.g., video cameras. They suggest to use different signaling mechanisms, such as QR codes, visual markers, or ultrasound for preference communication. QR codes and visual markers are also proposed by the Offlinetags [293] and TagMeNot [131] projects to prevent undesired picture or video recordings. Here the idea is that visual markers are detected by cameras and used, for instance, to blur or mask the user’s face in the recorded video stream.
Managing phone call interruptions

Further research has aimed to reduce interruptions caused by phone calls. Most existing approaches [61, 354, 362, 467] require persons being called to share their own context information (e.g., location, appointments, or activity) with callers in order to inform when to place a call. However, while these approaches can enhance territorial privacy by mitigating undesired disturbances, sharing of one’s own context poses a risk for a user’s information privacy. This tradeoff has already been investigated early on by Hudson and Smith [312] in the context of computer supported cooperative work. They stated, that “one person’s contextual awareness is another person’s lack of privacy” [312].

In contrast to requiring callees to share their context information, other approaches are based on the idea that callers share more detailed information about their call [533, 265]. Granidi et al. [265] propose that callers should have the option to share a call’s subject, expected length, urgency, and importance besides other information. Their work is based on their prior findings stemming from incoming call analysis [263]. A collaborative approach for call acceptance decisions is proposed by Marti and Schmandt [438] based on wireless finger rings. The rings vibrate on each incoming call in a group of conversation partners and each person can veto the call by touching their finger ring.

Khalil et al. [353] propose to automatically adapt phone settings based on calendar data. Phone sensors and wearable sensors have also been used to learn a user’s volume preferences for notifications about incoming calls, SMS, and calendar alarms [352, 304, 548, 712].

In contrast to related work, the privacy signaling module enables users to communicate privacy preferences to others in their proximity without requiring instrumentation of the environment or having to share personal context. While the signaling module does not allow for direct control, it is an optimistic fallback strategy in order to cope with situations in which no control points for enforcing privacy preferences could be discovered by any of the other discovery modules.

8.7 Summary

In this chapter we provided an overview of the discovery and enforcement modules in our proposed privacy framework. The modules address the different characteristics of the user’s current environment and involved privacy implications. Figure 8.33 provides an overview of our framework, showing the applicability of the proposed modules to different environments and their contributions to privacy awareness and control.

The personal device module is responsible for registering a user’s observable items, for the discovery of privacy implications stemming from personal devices, and for enforcing privacy decisions on those
devices. We have shown the feasibility of the module by integrating a privacy enforcement layer in the Android application framework.

The trusted environment module is the main component to allow privacy discovery and enforcement of entities in the user’s physical territory. One part of the module assumes the existence of a trusted infrastructure, which allows direct discovery and control in collaboration with individual entities. Other features of the module assume the existence of a trusted system that allows indirect control through the delegation of privacy enforcement according to a user’s privacy preferences. We assume to find trusted infrastructures and systems predominantly in personal and shared personal environments. However, shared environments (e.g., an office or school building) could likewise be equipped with such infrastructures and systems but might provide less control. The implementation of the module and the preliminary user study that was conducted as part of the ATRACO project showed the effectiveness and acceptance of the approach.

For discovering privacy implications in public environments we proposed the beacon-based discovery module and community-based discovery module. The first module assumes the collaboration of entities in order to provide reliable broadcasts of PriFi beacons. Our implementation of a lightweight prototype showed that entities could easily be equipped with the beaconing approach to communicate their channel policies. Because the proposed implementation of the module as part
of the privacy agent requires a patch of the WiFi stack, we proposed a fallback mechanism which is compatible with all Android devices.

In contrast to the beaconing approach the community-based discovery module does not require an entity’s collaboration. It assumes that privacy implications are collected by users in a crowd-sourced manner. We demonstrated the feasibility of the approach for the crowd-sourced collection of information about public video cameras. However, this crowd-sourced approach depends on the visibility of privacy implications, and thus is not readily applicable to entirely invisible UbiComp systems.

While enforcing privacy decisions depends on the availability of control points, we propose the privacy signaling module as a fallback strategy in situations without direct control. Such situations obtain primarily in shared or public environments with undesired disturbances stemming from other persons. The module allows to signal a user’s preferences to other entities nearby. The evaluation of our prototype has shown that the signaling approach is accepted and would be readily employed in several everyday situations.

The discovery and enforcement modules interact with the privacy engine, which holds the instantiation of the current privacy graph. The engine supports user-centered privacy management through a user interface for privacy awareness and control. The design and evaluation of this user interface will be discussed in the next chapter.
In this chapter, we discuss our iterative design process and evaluation of a user interface that supports privacy awareness and control for individual users. The user interface is an integral part of the privacy agent and is directly connected to the privacy engine, which provides access to the privacy graph (cf. Figure 8.1). Privacy awareness is supported by providing different views of current and past privacy implications that are extracted from the privacy graph and its history, respectively. These views further allow users to exert direct privacy control decisions. Indirect privacy control is supported by a privacy profile dialog, which allows users to create static or conditional profiles with individual privacy preferences.

The design process of our interface is primarily guided by the relevant factors for privacy awareness and control as discussed in Chapter 4. It is further supported by insights from existing work on user interfaces for privacy management, which we discuss in the next section. In Section 9.2 we outline several design challenges and requirements that have been considered and addressed in the iterative design process of the user interface, described in Section 9.3. The final prototype of the user interface is discussed in Section 9.4 followed by its evaluation in Section 9.5.

9.1 RELATED WORK

Existing user interfaces for supporting privacy awareness and control can be divided into three major categories: user interfaces for online privacy, for mobile privacy, and for UbiComp privacy. In addition to privacy-related user interfaces, there are also several tools for managing security threats. We discuss existing approaches in each of these categories in the following sections.

9.1.1 User interfaces for online privacy

With the development of P3P as a standardized and machine readable policy format for websites and online services (see Section 7.2), several tools have been proposed which aimed to support users in managing their privacy online. A first attempt was made by Cranor et al. [171] with their Privacy Bird user agent for P3P. The tool aims at making users aware of whether a website’s data handling practices matches the users’ self-configured privacy preferences. Immedi-
ate feedback of privacy preference compliance or violation is given in form of a bird icon with different speech bubbles, colors, and sounds.

Kelley et al. [349] proposed the privacy nutrition label for providing awareness about P3P policies in form of a grid view. The idea of the grid is to provide a quick overview of a website’s different purposes (listed in columns) for accessing personal data (listed in rows). Each cell in the grid indicates the privacy state by one of four icons, showing that the data 1) is used for this purpose, 2) is used unless the user opts-out, 3) is not used unless the user opts-in, or 4) is not used at all. A user study showed that the grid view performed better in making users aware of privacy issues than standard natural language privacy policies. Privacy control is not supported by the grid view.

The grid idea is extended by Angulo et al. [49] in their send data interface as part of the PrimeLife [522] project. Similar to the privacy nutrition label, purposes and accessed data are represented as columns and rows, respectively. However, the cells the of grid contain icons of one or more websites to signal the use of data for a specific purpose. Thus, the grid shows privacy implications from multiple websites in one view instead of having an individual view for each website as proposed by the privacy nutrition label approach. Furthermore, forwarding of data is indicated by an arrow symbol next to the website’s icon. However, it is not clear to whom the data is forwarded. The match or mismatch of privacy policies to configured privacy preferences is highlighted by a puzzle symbol together with textual descriptions of identified conflicts. The privacy preferences, to which policies should be matched, can be selected in the view from a drop down menu. Angulo et al. further propose to show privacy obligations (e.g., data retention) as part of a separate column at the end of the grid. However, this requires that obligations are applied by all websites listed in the row of a specified obligation.

Kolter and Pernul [364] proposed a configuration wizard which aims to support users in creating P3P conform privacy preferences. The wizard provides three different complexity modes in order to meet different demands of novices and experts. Configured privacy preferences can be browsed via the privacy cockpit, which again provides an overview in form of a grid view. However, this time columns indicate different service types of websites (e.g., online shopping or banking) for which preferences have been configured with the wizard. Rows represent the different configured privacy options. Their number depends on the chosen complexity mode. Columns of service types are ordered by their privacy impact determined by their configured privacy options. The privacy impact is further highlighted with gradual colored columns from red to yellow to green.

Kolter proposed the privacy cockpit as part of a user-centric privacy architecture [365], which also incorporates a user interface for visualizing past disclosures of personal data [363]. This data track tool
provides different views to support users in a recipient-based analysis, a temporal analysis, and a relation-based analysis of past data disclosures. A user study with 26 participants showed that their approach was accepted and would be used in different online scenarios.

There also exist several browser extensions that aim at providing awareness of privacy issues when being online. The Mozilla Lightbeam extension [464] offers a graph-based visualization of data flows to third parties while browsing websites. Similar to the privacy cockpit, it provides different views (graph, clock, and list) for analyzing third party connections. However, privacy awareness is limited to connection information and cookies, and does not provide information about what data is exchanged with third parties.

The PrivacyFix extension [60] provides a dashboard that highlights negative privacy settings for Google services, Twitter, and the online social networks Facebook and LinkedIn. The dashboard does further allow users to directly change those negative settings to more privacy-friendly configurations.

The widespread use of online social networks (OSNs) motivated the development of several user interfaces that aim to support users in efficiently managing access to personal information. The PViz interface [444] aims at managing groups and sub-groups of friends on different granularity levels by showing overlapping nodes of different size and intensity. Similarly, Egelman et al. [207] propose a privacy settings interface based on Venn diagrams in order to support access control decisions for intersecting groups. They further showed that users can be supported by giving them explicit feedback about potential privacy issues together with guidance of how to fix them.

Instant feedback about potential privacy issues or misconfigured privacy preferences has also been the focus of some other research. Lipford et al. [410] have shown that their audience-oriented view of profile information could significantly improve users’ understanding of their privacy settings. Similarly, Caine et al. [126] propose to support users’ privacy settings in OSNs by giving them feedback about the potential number of recipients. The Privacy Watcher is a browser extension proposed by Paul et al. [509], which supports better feedback and control of privacy on Facebook. They realize their interface by overlaying the original Facebook profile with colored borders to indicate the group of recipients. Additional control widgets further support the instant change of privacy settings.

Wang et al. [674] propose different designs of a privacy authorization dialog for apps on OSNs. The dialog is designed as a grid, based on the privacy nutrition label [349].
Several privacy awareness and control interfaces in the context of mobile computing focus on location privacy. Sadeh et al. [556] propose a web-based control interface as part of their PeopleFinder location sharing platform. The interface allows users to create location access rules for individuals or self-defined groups. Access rules can be further refined by time and location constraints, which can be specified as collections of rectangles on a map. Feedback is provided by pop up notifications whenever the user’s location is requested. An auditing view should further support users in refining their rules by enabling them to review past requests and to see which rules led to a grant or deny decision. Very similar user interfaces have been proposed by Toch et al. [649] as part of their Locaccino system. Scipioni and Langheinrich [578] suggest to share locations only for specific events and activities, which could be specified by location and a time period. Their prototype further allows to specify a group of recipients, to specify the shared location granularity, and to share the location only with persons in a specified proximity (e.g., closer than 1 km). Tsai et al. [653] limited the creation of location access rules to only time-based constraints. However, they found that participants preferred to also specify group-based rules.

Different privacy interfaces for specifying recipients and the granularity of shared sensor information on smartphones have been proposed by Christin et al. [155]. In an evaluation with 80 participants they found that their radar interface for granularity specification was preferred compared to a bar, slider, and “phone” interface. The radar interface represents each sensor data as a separate axis of the radar, and allows users to specify the shared granularity via three radio buttons on the axis with an increasing granularity to the center of the radar. In order to provide awareness of configured privacy settings they propose to extend the radar interface with picture-based warnings that illustrate privacy threats without the need of long textual descriptions [157]. Past sensor sharing and granularity of shared data can be additionally browsed in a history view.

Schlegel et al. [572] proposed an unobtrusive privacy awareness interface for smartphones. Their approach is based on eye symbols that are placed on the smartphone’s home screen. The number of eye symbols corresponds to the number of entities that access a user’s personal data. The size of symbols grows with the access frequency in order to allow users the identification of potential privacy issues. While this approach provides quick and simple privacy feedback, it lacks the capability to inform users about what is accessed, by whom it is accessed, and why it is accessed.

Several user interfaces have further been proposed for application-specific privacy management on smartphones. Kelley et al. [350] pro-
pose two alternative install dialogs for Android applications in order to more prominently present what personal data is accessed. However, their dialogs lacked information about the purpose of access, which was found to be important for users. Lin et al. [409] propose to extend Android’s permission view when installing new applications to show the purpose of sensitive resource access together with common expectations about permissions collected from other users. A similar collaborative approach is utilized by the XPrivacy [423] and ProtectMyPrivacy applications [37]. Both applications allow fine-grained control of applications’ resource access and provides crowdsourced settings recommendations.

As part of the Privacy Leaks prototype, Balebako et al. [70] developed two types of privacy awareness interfaces, which provide instant notifications when an app accesses sensitive data (e.g., the user’s location) and a grid based log view revealing the frequency of resource access for installed applications. A detail view further allows to see to whom data has been forwarded by a specific application. Similar notification-based approaches have also been investigated by Thompson et al. [646].

9.1.3 User interfaces for UbiComp privacy

Nguyen and Mynatt [476] propose Privacy Mirrors as one of the first privacy frameworks to make users aware of the collection, flow, and access history of personal information in UbiComp systems. The mirror metaphor refers to three different presentation levels of the interface, which enables users to see how others would see them: glance provides a quick privacy hint like walking along a mirror, look provides more information like standing in front of a mirror, and interactive provides the most detailed information about the privacy state.

The Privacy Badge has been proposed by Gisch et al. [252] as a privacy awareness interface based on the metaphor of radiation badges. The badge is assumed to be always visible as a small icon on the screen of a user’s handheld device to visualize the user’s current privacy state. Detailed information about privacy implications can be received by additional views of the badge, showing what has been accessed, by whom, and when. The accessed information is shown as one or more icons on three concentric rings around the user. The rings represent data categories of different sensitivity. Privacy control is supported by placing services and information to one of the three rings. Arranging services on the rings allows users to assess the trust of a service, which implicitly controls the access to information. In an extended version of the badge [247], users are also able to configure instant notifications of access and to view a service description before using a service.
Caine et al. [129] proposed the DigiSwitch, which is a medical system for elderly in form of a digital picture frame. The ambient device enables older adults to perceive what information is collected and shared with caregivers, and allows them to pause data forwarding for different parts of the system. A friend’s view further enables users to see exactly what caregivers are seeing. Their usability study revealed that older adults liked to control different sensing devices individually rather than switching off the whole system.

Christin et al. [156] proposed the concept of privacy bubbles, as a novel approach to control privacy in UbiComp content sharing applications. The bubbles present private spheres which are limited by time and space in order to enforce access to shared content. For instance, to enable access to pictures taken at a specific event only to persons that have been to the event as well. The control interface allows to configure the radius of the bubble and its duration.

### 9.1.4 Security related user interfaces

Consolvo et al. [164] created the WiFi Privacy Ticker, an awareness interface for personal computers, which shows users when private information is transmitted over an unencrypted WiFi connection. In order to allow the monitoring of traffic, users have to preconfigure sensitive information (limited to simple terms, e.g., an email address or a credit card number) and set its sensitivity level.

As part of a peer-to-peer file sharing prototype, Rode et al. [538] propose a pie-based user interface, which visualizes system activity and supports users in access control management of their files. Different users are represented as individual colored slices of the pie. Access restrictions are represented as multiple concentric regions of the pie in which users can place their files in form of colored dots.

The expandable grid has been proposed by Reeder et al. [531] as a management interface for several types of security policies. The visualization approach is based on an interactive matrix. However, a user study revealed that their proposed approach is too complex for novice users. Based on the study results, they derived several design guidelines, which have been respected by the latter work on privacy nutrition labels [349] described above. The most relevant guidelines are: provide a starting point, provide a summary display, use short labels, place one dimension per axis, provide plenty of explanation for icons, and emphasize or eliminate interactivity.

Several other awareness and control interfaces for expert users have been proposed in the field of network security. Ball et al. [71] use a grid layout to visualize communication patterns between home devices and external hosts. Mansmann et al. [430] propose a hierarchical sunburst visualization in order to support network administrators in understanding and configuring firewall settings.
The AlertWheel [201] is a more sophisticated radial visualization for analyzing security related network events leveraging new ways of displaying bipartite graphs. Radial visualization approaches for network security analysis have also been proposed for the VisAlert [236] and MalwareVis [709] user interfaces. Fischer et al. [228] propose different map-based, glyph-based, and graph-based visualization techniques as part of their VisTracer tool for the analysis of traceroute data.

9.2 DESIGN CHALLENGES AND REQUIREMENTS

The design of a holistic user interface for privacy awareness and control in UbiComp poses several challenges. We discuss these challenges for awareness and control separately, together with the identified requirements that we followed in our iterative design process.

9.2.1 Providing awareness

Based on the results of our literature review and own studies on privacy influencing factors in Chapter 4, a privacy user interface should make users aware of who affects their privacy, how it is affected, and why it is affected. With respect to our territorial privacy model (see Section 3.2.4) this involves the following information:
WHO

- entities (persons, stakeholders, devices, applications, services)
- entities’ presence in the user’s territories (personal, physical, virtual extended)

HOW

- observations (content, information type, granularity)
- disturbances (notification, interaction, automation)
- dependencies between observations and disturbances
- conditions (context)
- obligations (details of observation and disturbance handling)

WHY

- purpose of observations and disturbances
- utility and own benefit

Due to the potentially high complexity of UbiComp scenarios and the multitude of involved privacy implications, one design challenge is the presentation of this information in a concise way to prevent informational overload. Therefore, according to Shneiderman’s [592] “visual information-seeking mantra”, it is required to provide an initial overview, zoom and filter options, as well as further views which provide details on demand. The displayed information on different granularity levels should respect the relevance of privacy influencing factors. Therefore, the high-level overview should focus on offering information about privacy-affecting entities and the type of privacy implications, while more detailed information (such as the purpose, conditions, and obligations) should be provided in additional views.

Another challenge for the design of an awareness interface is the pervasiveness of privacy implications stemming from invisible UbiComp systems. Privacy implications can occur in any everyday situation and are especially hard to perceive when users are not actively engaged in system interactions. While users could be notified about new privacy implications, this poses the risk of annoying interruptions, which again could be perceived as undesired disturbances of one’s privacy. Delivering privacy warnings in an acceptable manner requires appropriate timing and knowledge about the seriousness of privacy implications. The design of effective warning dialogs should further respect the six design guidelines proposed by Bauer et al. [77]: 1) describe the risk comprehensively, 2) be concise and accurate, 3) offer meaningful options, 4) present relevant contextual information, 5) present relevant auditing information, and 6) follow a consistent layout.
An alternative approach to providing instant awareness through privacy warnings could be based on a privacy history, which allows users to gain awareness at a later point in time. Therefore, the awareness interface is not only required to provide an overview of current privacy implications, but should also enable users to browse a history of past privacy implications. As shown by the related work on privacy interfaces in Section 9.1, a history view can further support users in identifying issues of their configured privacy preferences.

### 9.2.2 Providing control

In general, as suggested by the findings of Chapter 4, privacy control should be supported for the same factors of who, how, and why as discussed for providing awareness. Allowing control of all these factors supports coarse-grained control options (e.g., entity based or channel based control decisions), as well as fine-grained control options (e.g., controlling conditions or obligations). Especially coarse-grained controls (e.g., on/off switches) often provide the advantage of being simpler to understand and use [397].

Privacy control should be supported on two levels: direct control and indirect control. Direct control refers to explicit privacy decisions, which users should be able to manually exert in one of the awareness views of the privacy interface in order to control current privacy implications. Direct control is especially suited for coarse-grained control options. Indirect control refers to the specification of privacy preferences or privacy profiles, which define a set of coarse-grained and fine-grained privacy decisions for recurring situations. Profiles should be activatable either manually or automatically based on pre-defined context conditions.

The design challenges for providing direct control, lie in the effective support of user decisions and conflict handling. Depending on the available control points and selected control strategies of the privacy engine (see Section 6.4.2), the enforcement of direct control decisions might have undesired side effects. For instance, if in the running use case (see Section 5.5.1) Alice would not want the fitness app to receive her heart rate, and neither the app nor the application framework of the smartphone would provide control points for switching off the respective observation channel, the only available control point would be the wrist band itself. However, switching off the heart rate channel to the smartphone would also prevent the health application from detecting critical health states and calling first aid in case of an emergency. Such a conflict between desired privacy controls and potential undesired side effects needs to be considered in the design process of the user interface.

A further challenge is the support of privacy preference specification. As discussed in Section 3.2.3, privacy is often perceived as dy-
namic boundary regulation process and can depend on several context factors. Thus, a user interface for the management of privacy preferences should provide users with means of specifying conditional preferences based on context information. While such privacy preferences can become quite complex, it is required to reduce the management effort and to minimize errors in defining preferences. In the context of access control policies, Smetters and Good [601] propose a set of design guidelines, which could also be applied to privacy management: only allow positive grants of access, simplify the inheritance model for access control changes, limit the types of permissions that can be granted, and allow group definitions. We have respected these guidelines in our design process, which we discuss in the next section.

\section*{9.3 Design Process}

We followed a user-centered design process, which involved the creation and iterative refinement of several mockup prototypes, as well as three user studies with different prototypes of increasing functionality. The results of our preliminary studies guided the design of our final prototype, which has been evaluated in a more sophisticated user study with participants engaged in realistic scenarios.

In the following, we first discuss the initial mockups and first functional prototypes used in our preliminary user studies, followed by a discussion of the study results and lessons learned, which have been respected for the design of our final user interface.

\subsection*{9.3.1 Initial mockups}

At the beginning of the design process we developed several mockup user interfaces\footnote{Some mockups have been developed as part of the bachelor’s theses of David Thierbach [644] and Nelli Natan [469].}, which have been discussed in a small focus group of three privacy experts in order to refine the proposals and to select candidates for later usability studies. We discuss four of these mockups in the following sections: the radial awareness view, the block awareness view, the table awareness view, and the privacy profile view.

\textbf{Radial awareness view}

Motivated by related work proposing radial user interfaces (see Section 9.1) and the positive aspects associated with such approaches in terms of aesthetics, efficiency, and effectiveness [139, 192], we opted for a radial awareness view in our first mockups.

An example mockup of the radial awareness view for parts of the coming home use case is depicted in Figure 9.1. The basic idea of the view is to show privacy implications as part of a pie visualization...
Figure 9.1: Mockup of the radial privacy awareness view showing privacy implications of the coming home use case. Observation and disturbance channels are represented as pie slices. Entities are represented as cells of a slice and in the color of the respective territory (private, physical, or virtual).

around the user who is placed in the center of the view. Slices of the pie represent observation and disturbances channels. The content of an observation channel flows from the center to the outer edge of the pie, while the flow of disturbance channels is represented in the inverse direction towards the user. Entities are visualized as cells in a slice. For observation channels, inlying entities forward the channel’s content to their outlying neighbors. For disturbance channels, the disturbances of inlying entities are triggered or controlled by their outlying neighbors. The background’s saturation level of an entity’s cell indicates its current state. Cells of currently active observing or disturbing entities are shown in full saturation, while the cells of currently inactive entities show a lower saturation. An entity is referred to as inactive when it is associated with a conditional observation or disturbance (e.g., the location service will only have access to the location in case of an emergency). Further details of conditions, obligations, and the purpose associated with privacy implications are assumed to be provided via a separate view when selecting an entity cell. The boundary of the physical territory is indicated by a black border.

The color scheme of a previous mockup version supported the visual distinction of observation channels (orange) and disturbance channels (green). The source of observation channels and the sinks
of disturbance channels were colored in the channel’s color, while intermediate entities are colored gray. However, in initial focus group discussions with three privacy experts, it turned out that the distinction between observations and disturbances was found less important than the distinction between the different territories: personal, physical, and virtual extended (see Section 5.2). Therefore, the version of the mockup shown in Figure 9.1 provides a visual distinction between the three territories in green, orange, and red. This approach has the advantage of highlighting potentially more relevant privacy implications of virtual entities.

The main drawbacks of the radial awareness view are scalability issues when a large number of entities and channels are involved, and the required screen size to provide an acceptable overview, which makes the approach unsuited for today’s mobile devices with comparatively small-dimensioned screens.

**Table awareness view**

The table awareness view is motivated by the different grid-based approaches discussed in Section 9.1. The basic idea of the table view is the presentation of observations and disturbances in form of rows, and entities in form of columns. A mockup of the first design iteration is depicted in Figure 9.2, showing privacy implications of the coming home use case. Entities are grouped in the four categories sensors, actuators, services, and persons. The categories can be expanded through the triangle symbol to show included entities (as shown for sensors and services in Figure 9.2). A filled cell of the table indicates that the entity has access to an observation (green cell), or is involved in a
Figure 9.3: Mockup of the table view after the fifth design iteration, showing privacy implications of the coming home use case. Observations and disturbances are grouped by their purpose, entities are grouped by territory.

disturbance (orange cell). For collapsed categories, a filled cell indicates that at least one of the contained entities causes the respective privacy implication. Also observations and disturbances can be expanded to show dependencies. In Figure 9.2, the motion observation is forwarded to the smart home system (solid arrow), which requires this observation in order to infer the current activity (dashed arrow). Conditions, obligations, and the purpose of privacy implications have not been investigated in this first version of the table mockup. Furthermore, the view does not provide awareness of a user’s private, physical, and virtual territories. While it can be implicitly assumed that sensors and actuators must be in the personal or physical territory, services and persons could be located in all three territories.

In the next iterations of the table view mockups, we addressed the shortcomings of the first mockup version and proposed two alternative table views as the outcome of the fifth iteration cycle. The first alternative is shown in Figure 9.3. The main differences to the first mockup version are the grouping of observations and disturbances by purpose and the grouping of entities by territory. The three territories are ordered by their privacy impact from left (personal) to right (virtual), and are further indicated by different colors (two blue tone colors for the personal and physical territory, and a red color for the virtual territory). By default, all groups are collapsed and can be expanded by the plus symbol. Figure 9.3 shows the expanded view for
the purpose *activity support* and the *physical environment*. The source of observations and the sink of disturbances are represented by icons indicating the type of observation or disturbance. It is assumed that selecting a cell or icon provides a textual description of the privacy implications together with associated conditions and obligations.

The second alternative for the table view after the fifth iteration cycle is shown in Figure 9.4. The view was optimized for typical screen sizes of today’s smartphones, which is assumed to be the deployment platform of our privacy agent. Similar to the former approaches, a main view (Figure 9.4 left) provides an overview of all privacy implications. However, the main view is not grouped by purpose this time, but directly lists all observations and disturbances. Conditional implications are indicated with a gray cell. Selecting a row, column, or cell opens a more detailed view. The detail views after selecting the *physical environment* column and *personal device* column are depicted in the middle and right views of Figure 9.4, respectively. In a detail view, arrows show users the dependencies between privacy implications. If an arrow is directed to an entity that is not part of the current view (e.g., the forwarding channels in the personal device view), it is assumed that selecting an arrow switches to the territory view of the referenced entity. Conditions for inactive privacy implications are provided as textual descriptions of the respective cell.

![Mockup of the smartphone-optimized table awareness view. The main view (left) provides an overview of all privacy implications. Each row, column, or cell can be selected to provide a more detailed view. Selecting a column provides details about all containing entities as shown for the physical environment (middle) and personal devices (right).](image)
Figure 9.5: Mockup of the block-based awareness view. The main view a) shows existing observations in the top area (green), disturbances in the bottom area (orange), and purposes in the middle area. Selecting a purpose opens a detail view c) showing dependencies for this purpose. A basic history view b) shows past privacy implications.

**Block awareness view**

One drawback of the former grid-based views is the large amount of empty space used by non-filled cells. Therefore, in another iteration cycle of the purpose-centered table view shown in Figure 9.3, we opted for a block-based awareness view in order to present privacy implications in a more compact fashion. An example mockup of this block approach is depicted in Figure 9.5. The main view (a), is divided into three parts. The upper part shows current observations, the lower part shows current disturbances. A textual description of observations and disturbances is supported with stylized icons.

The middle part of the main view provides buttons for the different purposes of current privacy implications. Selecting a purpose opens a detail view showing the involved entities and dependencies between privacy implications for this purpose. In Figure 9.5 c), the purpose *activity support* has been selected. The green observation boxes are placed on top of the respective source entity (i.e., the sensor), orange disturbance boxes are placed under the respective sink entity (i.e., the actuator). Purpose details and dependencies of privacy implications are provided as textual descriptions at the top of the view.

In order to support users in browsing past privacy implications, additional left and right arrows around a calendar symbol allow to change the time window in which privacy implications should be pre-
The privacy control of the following items is particularly important for me:

- SMS
- mails
- pictures
- contacts
- calendar
- GPS sensor
- microphone
- display
- IMEI
- name
- notes
- heart rate
- motion sensor
- acceleration sensor
- incoming calls
- status messages
- acoustic disturb.
- haptic disturbances
- visual disturb.
- incoming msg. notif.

Figure 9.6: Participants’ ratings of the importance to control common observations and disturbances on mobile devices. Significant differences between women and men have been found for incoming message notifications only.

All of the discussed awareness views are assumed to provide direct control on different granularity levels. A privacy control decision can be exerted by a long touch (i.e., holding a button for more than a second) in all views. Depending on the selected button, this allows users to deny specific entities, observations, disturbances, or purposes. We further discuss possible direct control options when introducing the final prototype in Section 9.4.

Privacy profile management

In order to provide indirect control, users should be able to specify their privacy preferences in form of privacy profiles. As a first step in the design process of our profile management interface, we conducted an online survey to gather information about what users want to specify in their privacy profiles, and about the features a profile management interface should offer. Survey questions were motivated by our findings about privacy concerns discussed in Chapter 4.

The survey was completed by 43 persons (29 male, 14 female) with an average age of 26 years (MD=23). Most (27) persons were students from different subjects. First, participants rated the relevance of controlling typical observations and disturbances on mobile devices. The results, depicted in Figure 9.6, show that more than 90% of the participants found it particularly important to control access to their SMS, mails, pictures, and contacts. While also controlling access to the GPS sensor was important for most (82%) participants, access to heart rate, motion, or acceleration sensors was rated as less important. This might be due to the fact that those low level sensor data were consid-
A privacy profile should allow to specify settings about ... who has access to personal data
context condition for access
purpose of access
data handling  (use, store, forward)
storage retention

who has access to personal data
context condition for access
purpose of access
data handling  (use, store, forward)
storage retention

who has access to personal data
context condition for access
purpose of access

who disturbs (apps, services, persons)
context condition for disturbance
disturb.

Figure 9.7: Participants’ utility ratings for different profile specification features with respect to observations and disturbances.

Considered as rather uncritical for privacy and participants were not aware of what can be inferred from this data (e.g., the current activity and stress level). Another reason for this result might be the fact that heart rate sensors are typically worn only during sports, which might be considered less privacy critical. Controlling disturbances was mostly (93%) desired for acoustic disturbances, followed by the control of incoming phone calls (68%). Controlling visual disturbances was perceived as less important. While we could not find any gender specific differences for most observations and disturbances, we found a significant difference in the desire to control incoming message notifications. A Mann-Whitney U test (U=285.5, p=0.01413) revealed that women (79%) find it more important to control this kind of disturbance than men (38%).

We further asked participants to rate several features of privacy profiles. Figure 9.7 shows the results for participants’ ratings of different profile settings for observations and disturbances. Regarding observations, entities have been further distinguished between local apps, remote services, and other persons. For all three entity types, participants found it most relevant to control who has access to personal data, followed by controlling data handling practices and the purpose of access. While the specification of context conditions and storage retention for data access was rated lowest, it still is desired by most users (more than 80%). The relevance of features for controlling
disturbances was overall rated lower than for observations. However, still more than 70% of the participants would like privacy profiles to provide such features.

With respect to the specification of context conditions for access control, we asked users to rate the relevance of their own location, the time, their own activity, and a specific event as potential information for specifying contextual constraints. Further, users rated the utility of that context information for the automatic activation of privacy profiles. The results in Figure 9.8 show that the own location, a specific event, and the time were rated most relevant for specifying context constraints for access control as well as for the automatic activation of profiles. Interestingly, the own activity was rated lowest, especially for automatic profile activation. Furthermore, almost all participants (98%) desired manual profile activation and transparency of the current profile. The majority of participants also would like to get notified when a profile is activated (88%) and would like to give their consent before activation (76%). However, only 48% of the participants would like to get notified when a rule of the current profile applies, which highlights that too much feedback can lead to undesired disturbances and interruptions.

A first mockup of the privacy profile management interface supported by the findings of our online survey is depicted in Figure 9.9. The main view (Figure 9.9 left) lists existing profiles, allows to activate/deactivate a profile, the setting of context conditions for automatic profile activation, and to create new profiles. The profile view (Figure 9.9 middle) allows to edit a new or one of the existing profiles. Users can enter a profile name, can choose an icon for the profile, and can specify one or more rules.

Rules allow the definition of positive privacy-related access rights. With respect to our privacy model, a rule can be composed of the three main aspects of privacy implications: who, how, and why.

Figure 9.8: Utility ratings of different context information for automatic profile activation and conditional access control specifications.
Figure 9.9: Mockup of the privacy profile management interface. The main view (right) provides an overview of existing profiles and allows to activate/deactivate profiles. Profiles can be modified in the profile view (center) through creating one or more rules, that specify who should be allowed to affect privacy, how, and why (left).

In the rule view (Figure 9.9 right), users can edit these aspects according to their privacy needs for the current profile. The *who* part allows to specify one or more privacy-affecting entities from four categories: persons/groups, local apps, environmental systems, and remote services. These categories reflect the main entities involved in the different territory types, see Section 5.2. The *how* part allows users to specify allowed observations (*access my data*) and disturbances (*access my attention*). Additionally, users can set a *condition* in order to limit privacy implications to specific contexts (e.g., a location, activity, or time). Finally, a rule can define *why* privacy implications can occur by specifying a purpose. This would assure that entities (*who*) can cause observations and disturbances (*how*) only for the specified purpose.

Each button for the specification of who, how, and why, opens a list with possible items (e.g., possible persons, observations, or purposes). These lists are assumed to be filled with information collected during the discovery process, and per default show only current privacy implications in order to ease the specification of privacy profiles for the current situation. If the user wants to specify a profile for a different situation, she can optionally choose to show all known information.

**Functional prototypes**

In order to evaluate the effectiveness of our final mockups, we created different functional prototypes for subsequent usability tests. Because we assume a user’s mobile device to be the target platform for the privacy agent, we only implemented mockup prototypes that can be
realized for small screen sizes. Therefore, the radial awareness view was left out for usability studies.

We realized the table-based and block-based awareness views as websites and modeled the GUI elements as interactive SVG elements. This allowed us to run platform independent usability tests by loading the respective awareness views in the web browser of a mobile device. For the first awareness views we were only interested in their effectiveness of making users aware of potential privacy implications. Thus, the functionality of the awareness views was limited to the presentation of privacy implications. Direct control options were not yet integrated. The profile management view was implemented as an Android based prototype in order to cope with the higher dynamics of profile creation and modification.

9.3.2 User study: table view and block view

We conducted the first usability study with a functional prototype of the table-based awareness view shown in Figure 9.3, and a functional prototype of the block-based awareness view shown in Figure 9.5.

Methodology

The study followed a between-subjects design with two groups of 13 participants in each group. After participants provided demographic and smartphone usage information, they completed the Internet users’ information privacy concerns (IUIPC) questionnaire [426] in order to capture their general privacy attitudes towards the dimensions of collection, awareness, and control.

Participants were then briefly introduced to the respective interface (block-based or table-based) and subsequently performed 5 tasks with different complexity. Because the table view was not optimized for small smartphone screens, both interface approaches were presented on a tablet device (Samsung Galaxy Tab 10.1), see Figure 9.10. For both groups, the awareness view showed the privacy implications.

Figure 9.10: A Samsung tablet showing the main views of the block-based (left) and table-based (right) awareness interfaces as used in the user study.
of the running use case (see Section 5.5.1). Each task was scored with 6 or 7 points related to the number of correctly answered subitems of a task. Wrong answered subitems lead to a point being subtracted.

In the first task, participants had to identify all entities that have access to the heart rate. Task 2 asked for all observations that are required for the purpose of providing fitness statistics. In task 3, participants should identify the conditional privacy implications of the health app. This task was divided into identifying conditional observations (3a) and conditional disturbances (3b). In task 4 and 5, participants were asked to identify all existing observations and disturbances, respectively. Participants received a German version of the following textual task descriptions:

**Task 1** Please select the heart rate and state which personal devices can access your heart rate and which cannot.

**Task 2** Please select the exercise analysis and state what personal information is accessed in order to analyze your exercises.

**Task 3a** Please select the health app. Who can access information provided by the health app and on what condition?

**Task 3b** What are potential disturbances of the health app and on what condition do they occur?

**Task 4** Please name all personal information that could be accessed.

**Task 5** Please name all potential disturbances that could occur.

After each task, participants completed the ASQ questionnaire [404] in order to measure their task related satisfaction with the interface. The general usability of the UI was measured with the PSSUQ questionnaire [404] at the end of the study, followed by a short interview and questions about individual preferences of visualization aspects.

Each session lasted 20 minutes on average and was recorded on video in order to identify problems in the interaction process. Participants were rewarded with sweets and could optionally participate in a shopping voucher raffle.

**Participants**

All 26 participants were recruited from our university student population. The average age was 24 (MD=24, SD=3) with 9 female and 17 male participants. The gender-specific distribution per group was fairly equal (group table view: 5 female, 8 male | group block view: 4 female, 9 male). Most (21) had a computer science background. All but two participants (1 in each group) owned a smartphone. Most participants (14) stated to frequently use their smartphone, while 9 stated to use it only occasionally. Their privacy concerns, measured
Results: usability

The results for each task are depicted in Figure 9.11. Except for task 3, the median score of participants in the block view group was higher than of participants in the table view group. However, running a Mann-Whitney U test for each of the tasks revealed significant differences only for task 1 (U=141.5, p<.01). No significant differences have been found for the positive ASQ results, which reflects participants’ satisfaction with both user interfaces. Even though almost all participants in both groups were able to identify the conditional disturbances in task 3b (i.e., the vibration and acoustic warning in case of an irregular health state), most had trouble in identifying the conditional observations in task 3a. The reason for this was that conditions were only provided as textual descriptions (see Figure 9.12), which most participants did not realize in the first task (3a), but figured out in the second part of the task (3b). This highlights that conditional privacy implications should be visualized more conspicuously.

Participants’ overall satisfaction with the respective user interface is depicted in Figure 9.13, showing positive results for all dimensions of the PSSUQ usability scale. While again the medians of the block view group are slightly higher than those of the table view group, no significant differences could be found. The lower ratings and higher
Figure 9.12: Screenshots of the block-based (left) and table-based (right) awareness interfaces as used in the study, showing textual conditions of the health app, which were required to solve task 3.

Figure 9.13: PSSUQ ratings for the table-based view and block-based view on a 7-point Likert scale.

Variance for the system usefulness (SysUse) and interface quality (IntQual) of the table-based view show that this approach was perceived as more complex and thus less useful than the block-based view. In the following we discuss the qualitative user feedback, which can help to identify the shortcomings of the awareness views.

Results: user feedback

In the exit interview, participants were asked to mention positive and negative aspects of the respective the user interface. Common positive aspects, mentioned for both interface approaches, were the color concept for highlighting different privacy implications and territories, as well as the clear structure of the interface. Participants of the table-based view especially liked the column-based distinction of entities into the three territory types, which enables them to quickly identify privacy-affecting remote entities.
Negative aspects of the block-based view were primarily limited to minor bugs of the functional prototype (e.g., displaced icons or a slow response time caused by a reload of the website). Only one participant stated that he found the navigation not very intuitive, because it did not conform to more familiar GUIs. More negative aspects have been mentioned for the table-based view, which underlines the identified usability issues. A common concern was the navigation through columns and rows, which was not intuitive for most (7) participants. When all cells were collapsed, participants first had to expand respective columns and rows in order to identify the required information. Because rows have been grouped by purpose, participants were required to expand each purpose row in order to find out who is involved in a specific observation or disturbance. A further drawback of the approach was that a cell in the table-based view must be matched to a column description (the observation or disturbance) and a row heading (the entity). This process was found to be too cumbersome for participants. Participants of the block-based view, on the other hand, liked the direct flow visualization of privacy implications and that each entity was represented as a separate box in the view. These aspects have been respected for the design of the final user interface, described in Section 9.4.

Participants were further asked whether they would use the interface in everyday situations. Figure 9.14 shows that all participants of the block view group would likely use the app. However, only 7 participants of the table view group stated to likely use the app, which again highlights the lower perceived usefulness of this approach caused by the drawbacks discussed above. While this only expresses the intention to use the app rather than actual behavior, the overall rating gives us an indication which interfaces is perceived as more useful. Commonly mentioned situations in which participants would likely use the awareness interface were the installation/testing of new smartphone applications, when being in environments with audio or video recordings (e.g., public transport or public places), and when using online services (e.g., for navigation purposes).

In order to assess the different visualization aspects, we asked participants to sort these aspects according to their perceived relevance,
see Figure 9.15. The results show that in general, awareness of observations is perceived as more important than awareness of disturbances. This is in alignment with the previous findings about the relevance of privacy profile specification features, see Figure 9.7 in Section 9.3.1. For observations, participants found it most important to be aware of observations from remote services, followed by environmental systems, and remote persons. Observations and disturbances from personal devices were perceived as less important. These results highlight that the proposed territorial separation of the awareness views (personal, physical environment, and virtual environment) are important to visualize different levels of perceived privacy implications.

Regarding details of privacy implications, participants found the type of accessed personal data, the privacy-affecting entity, conditions, and the purpose most relevant. This is in alignment with the discussed findings about privacy influencing factors in Chapter 4. However, while participants had trouble in identifying textual conditions in both evaluated awareness views, the condition of privacy implications should be visualized more prominently. Interestingly, sensor based observations were perceived as less relevant. This shows that not the access to sensor data itself, but the potential access to inferred higher level data and associated privacy risks should be the focus of the awareness view.

9.3.3 User study: smartphone-optimized table view

The first versions of the block-based and table-based interfaces were not optimized for small displays and thus have been evaluated on a tablet device. However, because we assume that the privacy agent is deployed on a user’s personal device, we developed a smartphone-optimized version of the table view as described in Section 9.3.1 (see also Figure 9.4).
Because many UbiComp systems exist in the popular application domain of ambient assistant living (see Section 2.3.3), we evaluated this version of the table-based interface in a usability study with six elderly participants. The study was conducted with participants of the focus group session discussed in Section 4.7.

**Methodology**

After participants had discussed the three wrist band scenarios (S1: health monitoring, S2: positioning, S3: barrier-free phone calls) with several observations and disturbances (see Section 4.7), they were briefly introduced to the table-based awareness view. Each participant was then issued a smartphone (Android Galaxy Nexus) with the table awareness view showing privacy implications in the context of the discussed scenarios. Participants had to solve three tasks with the awareness view in 30 minutes. In the first task (T1), participants had to identify all privacy implications. That is, they were asked to mark all existing observations and disturbances as well as all entities that either have access to observations or could cause disturbances. In the second task (T2), participants were asked to identify when privacy implications can occur (never, always, or under specific conditions). The purpose of specific privacy implications was asked in the last task (T3). Each correct answer was rewarded with one point, wrong answers led to a point being subtracted. In total, participants could achieve 28 points.

After each task, participants completed the ASQ [404] questionnaire to measure participants’ satisfaction and perceived efficiency of the user interface. Due to time constraints and the focus group format of the study, the PSSUQ and IUIPC were not completed by participants. Instead, the study was closed with a 10 minutes discussion to receive qualitative feedback about the strengths and shortcomings of the user interface.

**Participants**

The six participants (2 female, 4 male) were between 65 and 76 years old (MD=69, SD=4). Three of them had a university degree, two completed vocational training, and one participant held a doctoral degree as the highest education. All of them were still living independently in their own homes, either alone (3) or with their partner (3). Furthermore, all participants have used a touch device before and five of them owned a smartphone or tablet device.

**Results**

The results for all three tasks are depicted in Figure 9.16. While best results were achieved for the first task, the low median score as well
as the negative results for task 2 and task 3 show that the user interface did not effectively support participants in correctly identifying all privacy implications. While the negative results of task 3 were primarily caused by the fact that participants ran out of time, the negative results of the condition task 2 were likely because of participants’ misconceptions of conditional privacy implications.

The final discussion with participants revealed that the user interface was perceived as too complex in general. It was filled with too many details: “The system is too complex. It must be simple like Micky Mouse. [...] I think the challenge here is to break it down so that every fool even at night at 2am can get it” (P8). Most participants agreed on this. Only one participant, with a background in information technology, liked the clear structure of the interface: “I find the interface very clear structured as well as analytically and consequently thought out. However, it assumes that users enjoy the handling of such devices and have some previous knowledge about it. I think it would be easier for some people to ask simple questions, e.g., “who currently receives my data”, and get a simple answer” (P4). The idea of a spoken dialog interface was positively accepted by other participants: “I would rather be able to make use of clear questions and answers than deal with the symbolics of this system” (P3).

The results show that a simpler user interface is required to support privacy awareness of elderly, especially for users with less experience in using mobile devices. While the proposed spoken dialog interface could pose a reasonable alternative, another solution could be to provide a higher abstraction level of the awareness view and hide details, such as involved sensors and actuators.

9.3.4 User study: privacy profile interface

The third preliminary usability study of our design process was conducted with the functional prototype of the privacy profile interface as illustrated in Figure 9.9. While the previous studies investigated
the effectiveness of the different approaches to make users aware of potential privacy implications, we now investigate the effectiveness of our approach to support users with indirect control by defining specific context-aware privacy profiles for different situations.

**Methodology**

At the beginning of the study, participants provided demographic information, smartphone usage information, and answered the IUIPC questionnaire \[426\] to capture their privacy attitudes. Afterwards they received a brief introduction to the involved concepts of privacy profiles and to the functionality of the profile management interface. The interface was installed on an Android smartphone (LG nexus 4).

Participants had to complete 6 tasks with increasing difficulty. As a warm-up, in the first task, participants were asked to manually activate the predefined profile *at work*. In task 2, participants had to view the settings of this profile and should answer eight questions about who is granted access, what can be accessed, for what purpose, and on what conditions. In task 3, participants should modify the profile to allow different data handling practices of an entity, to grant different types of disturbances, and to include another condition. A new rule should be created in task 4, which involved a conditional disturbance of three different entities. While the former tasks were composed of more detailed instructions, the two final tasks consisted of use case descriptions with involved privacy preferences of Alice in our running use case (task 5) and our coming home use case (task 6). Participants should create new privacy profiles with one or more rules that satisfy Alice’s preferences for the respective use case. The main challenge for participants was to match the textual preference descriptions on to the available features of a privacy profile without further instructions.

Participants completed the ASQ questionnaire \[404\] after each task and the PSSUQ \[404\] at the end of the study to measure participants’ satisfaction and the usability of our interface. In a final interview, participants were asked to mention positive and negative aspects of the interfaces as well as their attitude towards using it in everyday situations. The interaction with the user interface was recorded on video in order to identify common interaction issues. An individual session of the study took 74 minutes on average (MD=73, SD=11).

**Participants**

Participants were recruited from our university campus. In total 12 participants (2 female, 10 male) took part in the study from which 5 also participated in the online survey we conducted during the design process of the interface. The average age was 24 (MD=24, SD=2) and most (10) were computer science students. One participant stud-
ied mathematics and one did an apprenticeship as a qualified medical employee. Ten participants owned a smartphone of which 7 stated to use it frequently and 2 to use it occasionally. Participants’ privacy concerns, measured by the IUIPC [426], were again consistently high for all three privacy dimensions: collection (MD=6.25, SD=1.41), awareness (MD=6.67, SD=0.48), and control (MD=6.33, SD=1.12).

Results: usability

The usability results are depicted in Figure 9.17. While we can see that user satisfaction of task completion (ASQ ratings) slightly decreases with increasing task difficulty, the results of the most challenging tasks 5 and 6 are still reasonably satisfying. This shows that even the task completion time of more than 6 minutes on average for the last two tasks was perceived as acceptable by participants. Furthermore, the PSSUQ results are positive for all dimensions showing that the perceived usability of the interface is quite high. Only the interface’s information quality (InfoQual) could be improved.

While the results of the perceived usability scales are promising, the task correctness was not always satisfactory. We categorized task results in correct, incomplete, and incorrect results. A correct result fulfilled all requirements of the task, i.e., the respective profile grants the correct observations and disturbances, involves the correct entities, as well as correct conditions, purposes, and actions. While in some cases this could be achieved with more than one configuration, all possible configurations were respected. Incomplete results are lacking some of these settings, but do not involve wrong settings. Incorrect results refer to profiles that specify wrong privacy settings, e.g., a profile that grants access to the wrong entity or on wrong conditions.

The correctness of task results is depicted in Figure 9.18. The first two simple tasks were solved correctly by almost all participants. Only two participants reported the wrong purpose, which has been specified in the predefined profile. Also the modification of a profile and the creation of a new rule was solved correctly by most participants. However, three participants created a new rule in task 3, which
led to wrong results. A common mistake in task 4 was that participants (4) forgot the specification of a condition, which resulted in an incomplete rule. Similar mistakes were made in task 6, when participants had to create a new profile for the coming home use case. Most mistakes were made by participants when creating the new profile for the running use case in task 5. While Bob’s conditional access to the position (task 5a) was solved correctly by most (9) participants, only three participants correctly specified the settings for the fitness app (task 5b) and health app (task 5c), and only 5 participants could create correct rules for the emergency service. The worst result of task 5c was caused by participants’ misconception of how the emergency condition is detected. Most (8) did not realize that an emergency is detected by the health app and that it therefore always requires access to a user’s vital data. Those participants incorrectly limited the health app’s vital data access to emergencies, which would render the health app useless. Such mistakes could be mitigated by integrating awareness aspects in the profile management interface. For instance, the privacy engine could detect such misconfigurations by matching the user’s profile settings with the health app’s channel policies and warn the user about inappropriate configurations.

<table>
<thead>
<tr>
<th>task</th>
<th>correct</th>
<th>incomplete</th>
<th>incorrect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) manual profile activation</td>
<td>completed correctly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) view profile settings</td>
<td>completed correctly</td>
<td></td>
<td>mixed up purpose</td>
</tr>
<tr>
<td>3) modify profile settings</td>
<td>completed correctly</td>
<td></td>
<td>created new rule</td>
</tr>
<tr>
<td>4) create new rule</td>
<td>completed correctly</td>
<td>no condition</td>
<td>misc</td>
</tr>
<tr>
<td>5a) access of Bob to position when running</td>
<td>completed correctly</td>
<td>no cond.</td>
<td>misc</td>
</tr>
<tr>
<td>5b) access of fitness app to position and vital data when running</td>
<td>completed correctly</td>
<td>no position</td>
<td>no vital data</td>
</tr>
<tr>
<td>5c) access of health app to position and vital data</td>
<td>completed correctly</td>
<td>no position</td>
<td>access limited to emergency</td>
</tr>
<tr>
<td>5d) access of emergency service to position and vital data in case of an emergency</td>
<td>completed correctly</td>
<td>forgot entity</td>
<td>misc</td>
</tr>
<tr>
<td>6a) access of smart home system to observations</td>
<td>completed correctly</td>
<td>no condition</td>
<td>misc</td>
</tr>
<tr>
<td>6b) block phone calls of colleagues</td>
<td>completed correctly</td>
<td>no condition</td>
<td></td>
</tr>
<tr>
<td>6c) indicate notifications by a blinking light</td>
<td>completed correctly</td>
<td>no condition</td>
<td>forg. entity</td>
</tr>
</tbody>
</table>
Results: user feedback

In the final interviews, participants provided qualitative feedback about positive and negative aspects of the interfaces as well as their attitudes towards using it in the proposed or other everyday situations. Most (10) participants found the interface well structured and easy to use. Five participants stated to like the variety of configuration features and the concept of specifying multiple rules per profile.

Negative aspects mentioned primarily concerned the lack of a help or documentation about configuration features. However, several (4) participants stated that such type of software typical requires some settling-in period in order to learn and better understand the features of the interface. However, we must note that almost all participants had a computer science background and therefore more expertise than typical users. Thus, the user interface should provide helpful instructions on the first use and more explanations in order to help novice users in efficiently creating correct privacy profiles.

All users stated to likely use the profile manager in the proposed running use case, coming home use cases, or similar everyday situations. While some participants would not specify such profiles for running, they mentioned hiking, mountain biking, or sports in general as other situations of specifying conditional privacy profiles in order to allow access in emergencies. In the coming home use case, almost all participants particularly liked the possibility to limit undesired disturbances. Only one participant stated that he would not specify profiles at home, because situations at home would be too dynamic and thus not allow to create a universal profile.

9.3.5 Discussion

The results of our first user studies revealed several insights, which guided the design of the final user interface for privacy awareness and control. Participants liked the clear structure of the table-based and block-based views as well as the color concept for highlighting privacy implications of different relevance. In the table-based view, especially the clear distinction of the three territory types (personal, physical, virtual) was positively commented on by participants. However, the navigation through rows and columns in order to identify the meaning of a cell in the table-based view, was perceived as cumbersome. This issue was also reflected in the slightly lower scores of completed tasks compared to the results of the block-based view, even though only the scores of one task differed significantly. A commonly mentioned positive aspect of the block-based view, was the simple visualization of information flows, which shows that this approach should be adopted for the final user interface design.

Our second study, in which we evaluated the usability of our modified table-based view within a group of older adults, showed that
this approach was perceived as far too complex and a simpler and more abstract solution is required for users of this target group. Especially details (e.g., active sensors which are the source of observations) were perceived as unnecessary information. Thus, for elderly, a user interface could be limited to provide awareness only of privacy implications in the virtual extended territory. While the usability study was conducted only with six participants, further research is required to investigate the effectiveness of a different approach with a larger group of older adults. However, for the scope of this thesis, we limit our further investigations on creating an effective user interface for users of younger generations as the main target group.

The usability results of the privacy profile interface suggest that our approach can effectively support users in creating context-aware privacy profiles for different situations. While the results are promising and user feedback confirmed the potential utility in everyday situations, the specification of privacy preferences in real situations is often more challenging than expected by users [508]. Therefore, the feasibility of our approach should further be investigated in a real world setup with users specifying privacy preferences for real situations.

In general, the results of all three user studies suggest that observations are perceived as more relevant than disturbances. Due to the current popularity of information privacy issues in press and media, this result is not surprising. However, the perceived relevance of privacy-affecting disturbances might increase prospectively with the growing number of automation and interaction technologies in our environments. As indicated by participants’ feedback in our third study, especially the home is a place where undesired disturbances are perceived as relevant. Thus, disturbances from home automation or multimedia systems at home might further increase users’ perceived relevance of disturbances.

9.4 THE PRIVIS APP

In the following sections we discuss the design, implementation, and evaluation of the final user interface for privacy awareness and control, called PriVis app (Privacy Visualization app). The design was guided by the results of the previous usability studies and aims at combining the positive aspects of our several preliminary proposals.

9.4.1 Overview

The final user interface (PriVis app) provides a comprehensive solution for user-centric privacy management in form of an awareness view, which offers direct control capabilities, a privacy history view, which allows the browsing of past privacy implications, and a profile management view, which allows users to specify their privacy prefer-
Figure 9.19: Final user interface for privacy awareness and control (PriVis app). From the main view a), users can navigate to the awareness view b), history view c), and the profile management view.

ences. Figure 9.19 depicts three Mockups of the final user interface. From the main view, users can navigate to the awareness and control view, the history view, and the profile management view. Each view is introduced with a brief description and a descriptive icon.

The awareness view and history view were designed as a combination of the positive aspects of the table-based and block-based approaches discussed in the previous sections. Their general structure is again based on a table layout, because it enables a quick navigation and was found to be more suitable for smaller screens. Observations and disturbances are represented as blue rows. Assuming an imaginary user to be located on the left of the screen, observations flow from the left to the right and disturbances from the right to the left, which is indicated by small arrows in each row. However, in contrast to the previous table-based approaches, columns do not represent entities but only the three territories (personal, physical, virtual extended), which was found to be a positive aspect of the table-based view. The different levels of privacy risks associated with each of these territories, are highlighted by a traffic light color scheme. For a better user understanding of the territory concept in the user interface, we describe entities as personal entities (i.e., entities in the personal territory), ambient entities (i.e., entities in the physical territory), and remote entities (i.e., entities in the virtual extended territory).
Figure 9.20: Final UI mockups showing the dependency view of the dynamic & sensor data category a), b) and of the notification & warnings category c) with privacy implications of the running use case.

9.4.2 Supporting privacy awareness

In order to support users’ different preferences for the presented details of privacy implications, the awareness view provides three abstraction layers: an entity summary, a dependency overview, and entity details. By default, the awareness view is started with the entity summary, shown in Figure 9.19 b). The view summarizes privacy implications by indicating which entities (personal, ambient, remote) currently cause observations and disturbances. Observations are grouped into dynamic & sensor data and static data. The first category refers to all observations stemming from sensors and to higher level dynamic information that can be inferred by sensors or by a combination of other observations (e.g., location, heart rate, activity, or health state). Static data refers to all personal data that is not subject to dynamic changes (e.g., contact information, personal messages, or pictures). Disturbances are grouped into notifications & interactions and automations & noise. The group of notifications and interactions refers to all disturbances that are directed to the user and thus request the user’s attention. Automations and noise refers to all other disturbances that might occur in the user’s physical proximity, e.g., by home automation devices, environmental systems, or other persons.

The existence of one or more active entities of one type (personal, ambient, or remote) is indicated with a full colored cell in the row of the respective observation or disturbance group (e.g., all cells of dynamic and sensor data in Figure 9.19 b). The number of active entities is shown in the center of the respective cell. If there currently
exist only inactive entities of a given type and group of observations/disturbances, a cell is colored with a lower saturation (e.g., the cell of remote entities for static data observations in Figure 9.19 b). To prevent information overload, the number of inactive entities is not shown in a cell. However, the summary at the bottom of the view shows the cumulative number of active and inactive entities for each of the three types. If no active entity exists for a group of observations/disturbances at all, the complete row is displayed with a lower saturation (e.g., the row of notifications and interactions).

Per default, the entity summary view shows the privacy implications that have been discovered by one of our proposed modules (see Chapter 8) during the last five minutes. To browse privacy implications of the past, the privacy history view (Figure 9.19 c) allows users to choose one of the three predefined time periods (last hour, today, yesterday), or to specify a custom period. The visualization of past privacy implications is realized in the same way as in the previously described summary view.

Selecting a row in the summary view opens the overview of dependencies. Figure 9.20 shows this overview for privacy implications of the running use case. Each observation and disturbance channel is represented as a row. Entities are represented as boxes in a table cell in order to allow the direct visualization of information flow and dependencies similar to the block-based view (see Section 9.3.1). As in the summary view, the flow of observations is from the left to the right (i.e., right entities depend on entities on their left) and inversely for disturbances (i.e., left entities depend on entities on their right).

The channel content is provided in form of an icon and a textual description in the first row of the table. The main area of the table view supports scrolling through channels and entities. The area can be ex-
Figure 9.22: The detail view a) of an entity (here the health app) lists all existing observation and disturbance channels. By selecting a specific purpose from a drop down menu b), the view can be filtered to show only involved privacy implications for this purpose c).

...
The detail view can be filtered by showing only involved channels of a specific purpose, which can be selected from a drop down menu at the bottom of the view (Figures 9.22 b and c). This feature is particularly interesting when users want to find out what information is required by entities that infer new observation channels, e.g., by filtering for the purpose infer locomotion of the fitness app or filtering for the purpose infer stress level of the health app.

### 9.4.3 Supporting privacy control

From the dependency view and detail view, users can open a purpose and control dialog by holding an entity or channel button for more than a second. When an entity has been selected, e.g., in Figure 9.23 a) the health app in the row of the heart rate observation channel, the dialog provides an overview of access conditions and of all involved purposes for the respective channel. Whether an access condition is currently fulfilled is indicated by a yes/no label next to the condition’s description. Furthermore, a user can directly control an entity’s access to the channel or deny any of the listed purposes by unchecking the respective check box. The list of purposes consists of all local purposes of the entity and all depending purposes of other entities that have been determined by the privacy engine through the discovery of channel policies (see Section 7). When the user denies a purpose that...
is required for other purposes, the user is warned through a short dialog which other purposes would be affected (see Figure 9.23 c).

When a channel has been selected in the dependency view, the purpose and control dialog shows all involved purposes for this channel and allows to globally control access to the channel for all entities (e.g., for the location observation channel as shown in Figure 9.23 b). If access to a channel has been denied for an entity or for a complete channel, the affected entities are highlighted in the dependency view with a solid red border (see Figure 9.23 d). If only one or more purposes have been denied, the entity is highlighted with a dashed red border. Denying a purpose or an entity will trigger the privacy engine to start the enforcement process in order to identify appropriate control points for the user’s privacy decision (see Section 6.4.2). Privacy is enforced through the identified control points by the respective enforcement module as discussed in Chapter 8.

---

Figure 9.24: Final mockups of the privacy profile management view. The design is mostly adopted from the previous prototype with a profile overview a), a profile modification view b), and a rule modification view c).

Figure 9.25: The app menu allows the in situ creation of a new privacy profile in the summary view a), in a dependency view b), and in an entity view c) based on the current settings of the respective view.
Indirect control is offered by the privacy profile view, which can be opened from the main view (see Figure 9.19). Due to the positive results of our usability study with the early prototype of this view (see Section 9.3.4), we adopted the general design and interaction concepts of the previous interface with a profile overview, a profile modification view, and a rule modification view, as shown in Figure 9.24.

In addition to the manual specification of privacy profiles, the user interface allows the creation of new profiles from the summary view, from a dependency view, and from an entity view via the application’s menu (see Figure 9.25). A profile that is created this way will automatically grant access to all visible entities and for all visible channels in the current view, except for channels and entities that have been denied by direct control decisions of the user. Thus, while such a profile reflects the current view it poses a simple alternative to create a profile with little effort. We assume that this approach of in situ profile creation will support users in specifying their privacy profiles more efficiently, because the privacy implications are related to the current situation.

9.4.4 Implementation

We implemented the final user interface as an Android application optimized for the 2014 Google developer phone (Nexus 5). The integration of the user interface in the overall architecture of the privacy agent is depicted in Figure 9.26. The different views have been implemented as individual Android Activities [259]. The privacy engine
provides an interface to current privacy implications, which are visualized in one of the three awareness views (summary view, dependency view, entity view). The history of the privacy graph is stored in a MySQL database, which is accessed by the privacy history view in order to visualize past privacy implications. Privacy profiles are stored in a MySQL database as well. Profiles can be manually created and modified in the privacy profile view. The semi-automatic creation of profiles through the awareness view is not yet supported in the current implementation of the prototype. We evaluated the usability and effectiveness of our PriVis app prototype in a lab study with real system components of our three discussed use cases. We discuss the design and results of our evaluation in the following section.

9.5 Evaluation

We evaluated the final prototype in a lab study with a selection of UbiComp technologies from our discussed use cases, see Section 5.5. We chose five technologies that represent the most popular UbiComp domains for individuals (health care, fitness, and smart home) and involve different privacy implications in form of observations and disturbances. Furthermore, the selected technologies provide a combination of already existing technologies and UbiComp technologies expected in the near future:

1. sensor wrist band with health app
2. sensor wrist band with fitness app
3. automatic door unlock system
4. cleaning robot
5. activity support system

We implemented functional prototypes of each of these technologies in order to embed them in a realistic scenario, which could be experienced by participants. The scenario was realized in a seminar room of our institute, which was assumed to be a shared smart apartment. The study setup is depicted in Figure 9.27. In the following, we first discuss the functional prototypes and their involved privacy implications followed by a description of our study methodology and a discussion of the study results.

9.5.1 Functional prototypes of UbiComp technologies

For the sensor wrist band we used an Empatica E3 [213] (see Figure 9.28 a), which is equipped with an optical heart rate sensor, and further sensors for temperature, skin conductance and acceleration.
The wrist band provides live streaming of sensor data via Bluetooth LE, which can be accessed by applications through a developer API for iOS and Android. Because we assumed the user smartphone to be a LG Nexus 5 for our evaluation, we developed Android versions of the health app and fitness app utilizing the Android API to receive sensor data from the Empatica wrist band, see Figure 9.28 b).

The health app provides a simple live view of vital parameters (heart rate, temperature, and skin conductance) and shows the calculated health state based on these parameters (see Figure 9.29 top). While the functional prototype uses only a simple algorithm to calculate the current health state based on static thresholds of heart rate and temperature, we informed participants that the health app calculates the health state by also respecting acceleration data and the user’s current stress level. In case of a critical health state, the health app was assumed to warn the user through the wrist band’s vibration motor. In case of a life-threatening health state, the health app was assumed to call first aid by forwarding the user’s current position and health state to an emergency service. In the settings dialog of the health app users could provide further personal data, such
as name, email address, and insurance number, and could enable or
disable the warning on critical health states and the calling of first
aid. Details about data handling practices could be found in a textual
privacy policy, which could be opened in the settings dialog.

The fitness app was assumed to calculate the user’s current locomo-
tion based on data from the wrist band (i.e., if the user is sitting, stand-
ing, walking or running) and provides a view of daily statistics for
fitness motivation (see Figure 9.29 bottom). In order to provide a re-
liable detection of participants’ current locomotion we implemented
the application as a Wizard of Oz prototype that was connected via
Bluetooth to the smartphone of the study supervisor. The fitness app
was assumed to backup fitness statistics on a central server and to
provide live sharing of the current locomotion with Facebook friends
for social motivation. Per default, the backup and live sharing fea-
tures were enabled. However, the latter one only applies when the
smartphone is connected via WiFi. These features could be config-
ured in the app’s settings dialog. Details about the features and in-
volved data handling practices of the fitness app were provided by a
textual privacy policy similar to the health app. Even though a recent
Figure 9.30: Functional prototype of the automatic door unlock system a) and the PriFi-enabled cleaning robot with a remote control b).

study [29] found that available fitness and health apps often (26% of free apps and 40% of paid apps from a total of 43 analyzed apps) do not provide any privacy policies, we opted for the integration of privacy policies in order to provide the highest level of privacy awareness that is typically given by mobile apps today. Our textual privacy policies are based on the privacy policies of a popular commercial health app and fitness app, and have only been modified to reflect the privacy implications of our scenario.

Both, the fitness app and the health app were integrated through the personal device module of the privacy agent (see Section 8.2) and thus all changes made in their respective settings dialogs were reflected in the PriVis app. In turn, control decisions made in the PriVis app were reflected in the settings dialog through control points provided by the applications.

The automatic door opening system (see Figure 9.30 a) detected the presence of a user through the received WiFi signal strength of the user’s smartphone. When a user was detected in front of the door, a door display in form of a wall mounted smartphone showed a personalized welcome message with the participant’s name and played a door unlock sound in order to simulate the automatic door unlocking. The door system was assumed to forward the presence of a detected person to roommates of the apartment. Here, no further privacy notices were provided, which is similar to most of available commercial UbiComp products [513].

For the cleaning robot (see Figure 9.30 b) we used our prototype introduced in Section 8.4.2, which is based on an iRobot Roomba 581 equipped with a Raspberry Pi. The cleaning robot was assumed to automatically start its cleaning process when the electricity rate for
Figure 9.31: Functional prototype of the activity support system realized on a large-scale smart board. The webcam’s active state is indicated by a bright red circle a). Users can switch activity recognition off b), and see that support is configured for watching TV, cooking, and fitness exercises c).

subsequent recharging is low. The cleaning robot provided a control point that enabled users to directly control the device through the privacy agent, e.g., to switch it off when it starts cleaning. Furthermore, the cleaning robot could be controlled through hardware buttons on the robot’s top and through a remote control. Both, the door system and the cleaning robot communicated their channel policies via PriFi beacons (see Section 8.4.1).

The activity support system was realized as a website on a large smart board, see Figure 9.31. The website showed the state of the activity recognition (running or off) and allowed users to switch the activity support on or off (see Figure 9.31 b). Control decisions were synchronized with the PriVis app through the trusted environment module (see Section 8.3). Activity recognition was assumed to leverage video data and audio data of a central video camera, as well as acceleration data of the user’s wrist band. The central video camera was a Logitech Webcam Pro 9000, which was placed on top of the smart board (see Figure 9.31 a). The camera’s active state was indicated with a red circle light whenever activity recognition was running. The system was assumed to be configured in order to support only cooking, TV watching, and fitness activities by showing helpful information (e.g., cooking receipts or fitness exercises) on the smart board’s display (see Figure 9.31 c). Furthermore, it was assumed that the system is active only between 8am and 6pm every day.

While some of the discussed functional prototypes provide complex settings and privacy implications, it was our intention to create a realistic scenario with realistic privacy implications. This requires prototypes with the described level of complexity.
9.5.2 Methodology

The aim of our study was to evaluate the usability of our final prototype of the privacy agent (PriVis app) and its effect on the acceptance of the selected UbiComp technologies. With respect to this we defined the following research hypotheses:

H1 The PriVis app enables users to identify privacy implications.
H2 The PriVis app enables users to control privacy implications.
H3 The PriVis app increases perceived privacy awareness.
H4 The PriVis app increases perceived privacy control.
H5 The PriVis app increases acceptance of UbiComp technologies.

To investigate these research hypotheses we opted for a between subjects design with three independent groups of which each participant experienced the same scenario with the discussed technologies. The first group A (full) received the original version of the PriVis app with both awareness and control features. The second group B (no control) received a modified version of the PriVis app without control functionalities by hiding the checkboxes of the purpose and control dialogs (see Figure 9.23). The final control group C (no privacy agent) experienced the scenario without the PriVis app. In order to ensure the homogeneity between groups in terms of general privacy concerns, technical affinity, attitudes towards technology, gender, and age, participants completed an online survey before attending the study. We measured privacy concerns with the IUIPC scale [426], and technical affinity and attitudes towards technology with scales adopted from Spiekermann [614] and Beach et al. [79].

At the beginning of the study, participants signed a consent form and received a brief introduction to the study procedure. The goal of the study was claimed to be the investigation of user acceptance of smart technology. The main scenario was divided into four parts. After each part the scenario was paused and participants were given four tasks with a different level of complexity and difficulty as part of an interview. The tasks asked participants to identify or control specific privacy implications of the experienced technology. The interview was followed by a questionnaire which measured participants perceived usability of the PriVis app (for the first two groups with the ASQ scale [404]), perceived privacy concerns, perceived privacy awareness and control (based on scales proposed by Spiekermann [614]), perceived usefulness (based on Davis et al. [180]), and behavioral intention to use (based on Mick and Fournier [454]). After each part, participants were asked to read a textual description of the general system functionality and how it operated in the experienced scenario part before completing the questionnaire. This ensured that
we measured participants’ privacy concerns and usefulness of the cor-
rect functionality of the system and not of their eventually incorrect
mental models. The scenario was structured as follows:

1. First, participants were introduced to the sensor wrist band and
health app. They were asked to wear the wrist band for the du-
ration of the study and they should assume that they recently
got this technology for their own purposes. Next, participants
of the first two groups received a 10 minutes introduction to
the respective version of the PriVis app. After this part all par-
ticipants were supported by the study supervisor in solving the
first tasks. Participants of the first two groups were introduced
how to solve the tasks with the PriVis app, while participants
of the control group were introduced how to solve the tasks
with available information and control features of the health
app (e.g., with the textual privacy policies).

2. The second part started with an introduction of the fitness app.
Participants should assume that they recently installed this ap-
lication for their own fitness motivation. They then should as-
sume that they come home from a stressful day to their shared
apartment (the seminar room) where they live with their friends
Mike and Lisa. Participants walked down the corridor to the
apartment door and experienced the automatic door opening
system. The following tasks should be solved by participants:
   a) Which systems in your environment, remote services or
      persons currently access your position? What is the pur-
      pose of access? \([\text{complexity}=\text{medium}, \text{difficulty}=\text{medium}]\)
   b) Which inactive remote services or persons could access
      your position and on what condition?
      \([\text{complexity}=\text{high}, \text{difficulty}=\text{medium}]\)
   c) Through which sensor(s) is your current position or pres-
      ence detected? \([\text{complexity}=\text{medium}, \text{difficulty}=\text{high}]\)
   d) You don’t want to store your fitness statistics on the 4Your-
      Fitness server anymore. Change the respective settings.
      \([\text{complexity}=\text{low}, \text{difficulty}=\text{low}]\)

3. In the third part of the scenario, participants should assume
that they just arrived at their shared apartment and their room-
mates are not home yet. Participants were told that all present
technology in the seminar room should be assumed to be part
of their shared apartment. While the screen and video camera of
the activity support system were off in the first two parts of the
scenario they now were switched on so that participants could
notice the running system. In order to enhance participants’ im-
mersion in the scenario, they were told that this evening it is
their turn to cook for their roommates. Thus, they first needed to pick a receipt from the cooking book in the kitchen area (see Figure 9.27). While they were doing this, they received a text message from Mike which indicates that Mike knows if the participant is currently sitting, standing or walking (e.g., “Hi Sarah! Why are you sitting around so lazily? ;) I’ll be home late tonight, sorry.”). The intention of the message was to create a surprise effect. Mike knows this information because the fitness app forwards it to Facebook friends when connected to WiFi. The latter is true because the smartphone just connected to the apartment’s WiFi when participants arrived home. To realize this part we implemented a simple messaging application which could receive customized messages from the supervisor’s smartphone. The involved tasks were:

a) Who or what can access your activity (e.g., watching TV or cooking) and for what purpose? [complexity=low, difficulty=low]

b) What information/data is required for the recognition of your activity? [complexity=medium, difficulty=high]

c) Who or what can access the video stream of the video camera in your apartment and on what condition? [complexity=low, difficulty=low]

d) Which persons can access your locomotion (sitting, standing, walking) and on what condition? [complexity=high, difficulty=medium]

4. In the last scenario part participants were asked to take a seat on the sofa and assume to relax from the stressful day before starting to cook for their roommates. Participants were free to watch TV or read one of the available books. After a while the cleaning robot started its cleaning process. The tasks were:

a) Deactivate the cleaning robot. [complexity=low, difficulty=low]

b) Why did the robot start its cleaning process? [complexity=low, difficulty=medium]

c) Are there any further disturbances (acoustic or visual) that could be caused through systems in your environment? [complexity=medium, difficulty=medium]

d) You want to prevent further disturbances while you are relaxing. What would be your strategy to realize this? [complexity=medium, difficulty=high]

All participants experienced the same scenario as outlined above. We decided to not counter-balance the scenario parts in order to prevent breaking the story of the scenario and to ensure the same immersion in the scenario for all participants. Furthermore, also the tasks
Table 9.1: Tasks for each scenario part with their level of complexity, level of difficulty, and how participants were supported in task solving.

<table>
<thead>
<tr>
<th>task</th>
<th>complexity</th>
<th>difficulty</th>
<th>supported by</th>
</tr>
</thead>
<tbody>
<tr>
<td>2a) aware of loc. access &amp; purpose</td>
<td>medium</td>
<td>medium</td>
<td>PriVis app (A,B); automatic door opening &amp; welcome message</td>
</tr>
<tr>
<td>2b) aware of condition for loc. access</td>
<td>high</td>
<td>medium</td>
<td>PriVis app (A,B); textual privacy policies</td>
</tr>
<tr>
<td>2c) aware of sensors for location</td>
<td>medium</td>
<td>high</td>
<td>PriVis app (A,B); visual door sensor</td>
</tr>
<tr>
<td>2d) control fitness stats backup</td>
<td>low</td>
<td>low</td>
<td>PriVis app (A); fitness app settings dialog</td>
</tr>
<tr>
<td>3a) aware of activity access &amp; purpose</td>
<td>low</td>
<td>low</td>
<td>PriVis app (A,B); display of activity support system</td>
</tr>
<tr>
<td>3b) aware of how act. is recognized</td>
<td>medium</td>
<td>high</td>
<td>PriVis app (A,B); visual camera</td>
</tr>
<tr>
<td>3c) aware of video access &amp; condition</td>
<td>low</td>
<td>low</td>
<td>PriVis app (A,B); visual camera</td>
</tr>
<tr>
<td>3d) aware of locomotion access &amp; condition</td>
<td>high</td>
<td>medium</td>
<td>PriVis app (A,B); textual privacy policies</td>
</tr>
<tr>
<td>4a) control cleaning robot</td>
<td>low</td>
<td>low</td>
<td>PriVis app (A); roomba buttons; roomba remote</td>
</tr>
<tr>
<td>4b) aware of cleaning condition</td>
<td>low</td>
<td>medium</td>
<td>PriVis app (A,B)</td>
</tr>
<tr>
<td>4c) aware of further disturbances</td>
<td>medium</td>
<td>medium</td>
<td>PriVis app (A,B); display of activity support system; smartphone settings</td>
</tr>
<tr>
<td>4d) control of all disturbances</td>
<td>medium</td>
<td>high</td>
<td>PriVis app (A); roomba controls; display of activity support system; smartphone settings</td>
</tr>
</tbody>
</table>

were set in the same order because some tasks either depend on a previous task, or implicitly provide answers to a previous task. All tasks were given in verbal form as part of the interview.

The tasks were created in such a way that most tasks could be solved by all groups and some could only be solved by groups A and B, which have been equipped with the PriVis app (2a,2c,3b,3c,4b). This way we wanted to investigate how privacy concerns and user acceptance of participants in the control group differ between UbiComp systems that support privacy awareness and control through own user interfaces, and UbiComp systems that do not offer such interfaces. Table 9.1 provides an overview of each task with their associated level of complexity, level of difficulty, and how participants were supported in solving the task either with a version of the PriVis app.
(A or B), or with features of the experienced UbiComp system (important for group C). Note, that the level of difficulty primarily refers to the expected difficulty of solving a task for participants equipped with the PriVis app. We provide detailed screenshots of the PriVis app in Appendix C, which show how each task could be solved with the different features of the app.

After the scenario participants completed a questionnaire regarding their perceived usability and usefulness of the PriVis app (based on the PSSUQ [404] and scales proposed by Spiekermann [614]). Participants provided further qualitative feedback in a final interview. Each session was audio recorded to support the later analysis of the qualitative feedback. The duration of a complete session varied from 50 to 100 minutes (M=63, SD=11) and was rewarded with 10 Euros.

### 9.5.3 Participants

In total 30 participants (15 female, 15 male) took part in the study. They were recruited from the student population of our university campus. Their age ranged from 19 to 27 years (M=24, SD=2) and most (19) were studying computer science. Other study subjects were physics, mathematics, biology, psychology, and medicine. All participants owned a smartphone and most stated to use it frequently (16) or very frequently (11).

We distributed participants equally between the 3 groups respecting gender, study subjects, and the results of our previous online survey regarding participants’ general privacy concerns, technical affinity, and technology attitudes (see Figure 9.32). A Kruskal-Wallis test confirmed that there were no significant differences between the three groups. However, we found significant gender specific differences for technical affinity. A Mann-Whitney U test revealed that male partici-
pants were found to have a higher technical affinity than female participants ($U=83.5$, $p<.01$, $r=.58$). We compensated this difference by equally assigning 5 male and 5 female participants to each group.

In general the technical affinity was very high, which reflects participants’ backgrounds (see Figure 9.32). However, the result of the technological attitude scale shows that participants were not too euphoric about technology and also had skeptical attitudes towards it (high values reflect positive attitudes). While all of the IUIPC dimensions show that participants were highly concerned about their privacy, the awareness dimensions seems to be the most relevant.

9.5.4 Results

In the following we first present the results of the task interviews, followed by the results of the perceived usability and usefulness of the privacy agent (PriVis app). We further discuss its potential effects on the acceptance of the experienced UbiComp technologies and on participants’ privacy concerns.

Task completion time

In the interviews, which were held after each scenario part, we measured the task completion time of each subtask as a first quantitative measure. The measurement was started after the respective task question and was stopped when the participant stated to not have any further comments. If this was not explicitly stated by the participant, the interviewer asked for further comments (e.g., “Are there any further systems that could access your position?”). Therefore, the measured duration does not necessarily reflect the time to correctly solve a task but rather the time participants were willing to spend for a task if they were not sure about the correct solution/answer.

Figure 9.33 shows the distribution of the measured task completion time for all relevant scenario parts. Note that part 1 has not been considered in the figure because its tasks were completed together with the supervisor as part of the introduction.

A Kruskal Wallis test revealed a significant effect of the group on the completion duration of task 3a ($H(2)=15.01$, $p<.001$), task 3c ($H(2)=13.63$, $p<.005$), and task 4d ($H(2)=13.01$, $p<.005$). Post-hoc Mann-Whitney tests with Bonferroni correction showed that participants of group C (no privacy agent) required significantly longer to complete task 3a compared to participants of group A ($p<.005$, $r=.81$) and of group B ($p<.01$, $r=.69$), and also longer to complete task 3c compared to group A ($p<.005$, $r=.79$).

A reason for this might be the low level of difficulty of the tasks 3a (awareness of location access) and 3c (awareness of video access) for participants of group A and B. Most participants (17) of these groups efficiently used the PriVis app to answer the tasks and were
Figure 9.33: Boxplots of the task completion time for all three groups. Significant differences were found for tasks 3a), 3c), and 4d)

convinced that their answer was correct. On the other hand, participants of group C were uncertain how to solve these tasks and often guessed who can access their location or the video stream, and thus, required more time to complete the task.

While task 2d (control fitness stats backups) and 4a (control cleaning robot) were also simple tasks, we could not find a significant difference in their completion times. This is likely because the tasks were also easy for participants of group C. All participants of that group quickly found the control option in the settings dialog of the fitness app (task 2d) and a way to stop the cleaning robot (task 4a). Interestingly, participants of group B (PriVis app without control options) required the most time to stop the cleaning robot, because they often tried to find a control option in the user interface of the PriVis app. The same effect was observed for task 4d (prevent all further disturbances), where participants of group B required significantly longer to complete the task than participants of group A (p<.001, r=.78) and participants of group C (p<.05, r=.47). The desire for control options in the PriVis app was also reflected by qualitative feedback of group B in the task interviews and final interviews: “I thought I could control this [all disturbances] in the PriVis app, but I couldn’t figure out how. However, it would be really handy. Then I simply could turn off everything in my environment. That would be really cool!” (P15) “I first thought that I could block [the backup of the fitness app] in the PriVis app... too bad I couldn’t.” (P13) “I’m not sure if I would use the PriVis app, because I miss the option to control things.” (P23) “I really like the PriVis app, but it would be even better if I would have a block option.” (P13)

While for most tasks we did not find significant differences in the completion time, participants of group A and B often required a similar amount of time to solve more complex and difficult tasks correctly, compared to group C who often guessed incorrect answers. We discuss the task correctness and solving strategies in the next section.
The distribution of the task correctness between all three groups is depicted in Figure 9.34. For awareness tasks, we calculated the correctness as the relative number of correctly named privacy implications. For control tasks, it was calculated as the relative number of correctly conducted control decisions. Because group A and B were supported by the PriVis app in the awareness tasks, wrong answers were penalized with a negative point. Participants of group C were not penalized and thus could also guess answers. In the control tasks, only participants of group A were penalized on wrong control decisions. Thus, participants supported by the PriVis app received a more strict assessment.

The results show that participants supported by the PriVis app were able to correctly solve most of the tasks. Only task 2c (awareness of location sensors), 3b (awareness of how activity is recognized), and task 4c (awareness of further disturbances) were not solved correctly by all participants of group A and B. Because group B was not provided with control options, participants of that group were further not able to correctly solve task 4d (control of all disturbances). While most participants of group C correctly solved task 2d (control fitness stats backups) and task 4a (control cleaning robot), most had trouble in solving the other tasks, even those which were supported by textual privacy policies or other system features. Kruskal Wallis tests showed that the differences between groups were highly significant \( p<.001 \) for all tasks except for 2c, 2d, and 4a. Post-hoc Mann-Whitney tests with Bonferroni correction showed that participants of group A and B significantly performed better in task solving than participants of group C for task 2a \( p<.05 \), 2b \( p<.01 \), 3a \( p<.001 \), 3b \( p<.001 \), 3c \( p<.001 \), 3d \( p<.001 \), and 4b \( p<.001 \), which is also clearly evident from Figure 9.34. In task 4c, we found only a significant difference between group A and C \( p<.01, r=.73 \). In the final task 4d, participants of group A solved the task significantly better than those of group B \( p<.001, r=.91 \) and of group C \( p<.001, r=.91 \).
9.5 Evaluation

The results confirm that the privacy agent effectively enables users to identify and control privacy implications. Thus, we can accept our hypotheses H1 and H2. In the following, we discuss the task solving strategies for each task in detail. Quoted statements of participants have been informally translated from German to English.

**Task 2a**  All participants of group A and most (8) participants of group B efficiently solved the first task (awareness of who can currently access the location and for what purpose). However, 2 participants (P17, P23) of group B did not use the PriVis app in the beginning and thus guessed the answers. Participant P23 stated that she first thought that the PriVis app only works with the Health application. She realized its assistance at the beginning of task 3a.

Almost all (9) participants of group C correctly mentioned the door system and also 4 participants correctly speculated that their presence might be shared with their roommates even though there was no indication for that. Further potential receivers mentioned were application operators (P21), the emergency service (P6), hackers (P3), and other services such as FindMyPhone (P2).

**Task 2b**  The second task (awareness of conditional access to location) was solved by most (15) participants of group A and B correctly. However, 4 participants of group A only mentioned the emergency service but not the doctor as a receiver of the location in a life threatening situation, potentially because they thought that he is part of the emergency service. Again participant P23 did not use the PriVis app to solve the task until task 3a.

Almost all (9) participants of group C mentioned the emergency service or the doctor as a receiver in a health threatening situation. However, no one mentioned the 4YourFitness server, which receives the location as part of the backup functionality of the fitness app when the smartphone is connected to WiFi. Even though this was described in the textual privacy policy of the fitness app, only two participants (P2, P26) opened the policy view. However, P26 only quickly scanned the policy and assumed that the live-sharing feature might forward the location (while it is only for sharing the current locomotion). Participants P2 stated: “I might be able to figure it out here in the policies, but they are too long and there is no search option.” This attitude was also confirmed by P26 who stated: “Privacy policies are always too long. You just scan them. No one will read them completely. Who still takes the time to read them today?” Other participants speculated about who might be able to receive their location and mentioned mobile providers (2) and application developers (2).
Task 2c

In the third task, participants should figure out which sensors determined their location in the experienced scenario part. Only 9 participants of group A and B correctly answered this task by opening the respective detail views in the PriVis app. However, 6 participants only mentioned the GPS sensor and one participant only the WiFi detector. Three participants (P5, P8, P23) were not able to figure out any sensor with the PriVis app. This shows that the concept of visualizing sinks and sources of observations and disturbances requires further clarification to users of the PriVis app. Interestingly, the three participants that were not able to answer the question with the PriVis app did also not speculate about potential sensors.

In group C, six participants mentioned the GPS sensor and recognized the sensor at the door. However, only one of them correctly recognized WiFi as the sensing technology. Two of them assumed Bluetooth and one NFC as the sensing technology of the door sensor. Other sensors mentioned were mobile cell towers (4) and motion sensors (2). The answers reflect the technical background and high technical affinity of most participants.

Task 2d

In the last task of the second part, participants should prevent the fitness app from backing up their fitness statistics to the 4YourFitness server. Almost all participants (28) efficiently solved this task. While participants of group B and C disabled the backup option in the settings view of the fitness app, most (8) participants of group A used the PriVis app to disable the purpose “backup your fitness statistics”. Only one participant of group A (P22) disabled the option in the settings view of the fitness app, and one participant (P9) disabled location access for the 4YourFitness server in the PriVis app. While this was not the intended control decision, it would have a similar effect and thus was not penalized in task scoring.

While most participants (9) of group C correctly solved the task, one participant (P3) disabled the live-sharing feature and stated that he would further deactivate WiFi and mobile data connections on his smartphone. Furthermore, three participants of group C expressed concerns about the effectiveness of the setting: “I’m not sure if this option is for local or remote backups” (P7). “I would have doubts on whether I could trust these settings. This data could be valuable for others” (P12). “Because these settings are so simple, it is hard to believe in their effectiveness. If I would really own this app I would study the privacy policies” (P28).

Two participants already realized the live-sharing feature in this task: “What is this? Sharing locomotion with friends... I would disable this as well” (P30, group A). “What does live-sharing mean? I would look this up in the privacy policies” (P2, group C). While both participants wondered about the live-sharing feature, only P30 was supported by the PriVis app and was therefore instantly aware of the privacy implication and could express his privacy preference. On the other hand,
P2 was not aware of the involved implications and only expressed his strategy of how he would gain awareness. This demonstrates the advantages of the PriVis app in contrast to the common way of communicating privacy implications to users in form of textual policies.

**Task 3A** In the first task of part 3, participants should answer who currently can access their activity and for what purpose. It was clarified that activity was a higher semantic information and referred to activities such as cooking or watching TV. All participants of group A and B correctly solved this task with the help of the PriVis app.

Surprisingly, only two participants (P2, P28) of group C noticed the activity support system and only P2 correctly stated that it has access to his activity. Two other participants (P6, P21) only noticed the camera on top of the screen but did not notice the displayed hints: “Smart Apartment” and “activity recognition is running” (see Figure 9.31). Most participants (6) of group C incorrectly speculated that their roommates or friends have access to their current activity because Mike was able to see that they were sitting or standing. P28 concluded: “He probably knows it because of the video camera over there.” While we expected more participants to draw this wrong conclusion, we found that the activity support system and camera were overlooked by most participants even though both were prominently placed in the room (see Figure 9.27) and participants had been clearly instructed that all present technology belongs to their apartment. While this might be caused by the artificial atmosphere and environment of the lab study, it is still interesting that most participants were not aware of the system. This highlights the benefits of the PriVis app that was able to make participants of group A and B aware of its presence, as also reflected in some of their reactions: “Ah, this is the activity support system. I didn’t notice it before” (P9). Especially in UbiComp scenarios with entirely hidden systems, the capability of making users aware of such systems will become highly relevant.

**Task 3B** Most (13) participants of group A and B correctly applied the filter for the purpose “recognize activity” in the detail view of the smart apartment in order to figure out which information is required to infer their activity. However, the remaining seven participants did not apply the filter and just mentioned all observations, which was penalized in the task assessment.

Because most (8) participants of group C were not aware of the activity support system, they only speculated about how their activity was recognized. Five participants correctly mentioned a video camera as a possible input factor for activity recognition, even though only two of them noticed the camera. The two other correct input factors for activity recognition (acceleration of the wrist band and audio recording) have been guessed only by one participant (P6) of group C.
Other incorrectly mentioned input factors were the position (4), motion sensors (4) and the use of devices, e.g., a TV or computer (3).

**Task 3c** All participants supported by the PriVis app efficiently solved this task and correctly mentioned the time condition (between 8am and 6pm) for the access to the video stream. Because the video camera was now explicitly mentioned as part of the task description, some participants of group C were surprised: “Oh, I didn’t notice the camera” (P7). “Aha, so there is a camera!” (P26). In group C, mentioned entities that might have access to the camera were roommates (4), Mike (2), the emergency doctor (2), the service provider (2), the cleaning robot (1), and hackers (1). Only one participant of group C (P21) correctly mentioned the smart apartment as the only system with access to the video stream, because she noticed the hint on the screen, which shows the text “activity recognition is running”.

**Task 3d** In this task, participants should figure out on what conditions someone can access their locomotion (sitting, standing, walking). Because of the received message, almost all participants (28) stated Mike to have access to it. The complete answer to the question was given by most (18) participants of group A and B. Only two participants of group B had trouble in finding the correct access condition.

In group C, six participants opened the privacy policy view of the fitness app but only two of them (P6, P24) were able to find correct information and stated that Facebook friends receive the locomotion when the live-sharing feature is enabled. However, they did not mention the condition that WiFi must be enabled. This condition was correctly guessed by P7 and correctly identified by P21 via the WiFi option in the settings view of the fitness app (see Figure 9.29). Similar to P2’s comment in task 2b, the unwillingness to read textual privacy policies was confirmed by P28 who stated: “The privacy policies are too long. No one will read them.”

**Task 4a** Stopping the cleaning robot was correctly solved by almost all (29) participants. In group A, 5 participants disabled the robot via the PriVis app and 5 directly by the button on its surface. Most (8) participants of group B, first tried to find a way to disable the cleaning robot via the PriVis app (version without control options). While most of them realized that this is not possible and directly controlled the robot, one participant (P18) gave up after she tried to figure it out with the PriVis app for three minutes: “I found it but I don’t know how to switch it off!” Only one participant of group B used the remote to stop the cleaning robot. Interestingly, in group C one half of participants used the remote and the other half the surface button to stop the robot. This suggests that participants without the PriVis app payed more attention to potential control options in
their environment. However, some participants of group C did also express the desire for a smartphone-based control solution, e.g., P6: “Is there an app for that? This would be helpful!”

**Task 4B** The reason (condition) why the cleaning robot started (the low electricity rate for recharging) was correctly identified by almost all (19) participants of group A and B. Only P27 did not find the information in the PriVis app. Participants of group C could only speculate about the reason. Most frequently mentioned reasons were a configured time schedule (7) and the fact that one was sitting on the couch and not standing in its way. Two participants ironically stated: “Because Mike wants to bug me” (P12, P16). Most (7) participants of group C further expressed their displeasure about the cleaning robot, e.g.: “This should not happen” (P2). “I find it disturbing when I’m sitting on the couch” (P3). “I would not want this” (P11). “That’s stupid. I want to read and relax” (21). “I want to have my peace at home” (P28).

**Task 4C** In this task participants were supposed to mention further potential disturbances. In group A and B, ten participants correctly solved this task and looked up the information in the two disturbance category views of the PriVis app. However, 7 participants only looked in the “automations & noise” category view, and thus did not mention the activity support system. Three participants were not able to find further disturbances. Either because they did not use the PriVis app for this task (P23, P25), or because of a misconception of the correct category view (P29).

In group C, only 3 participants (P2, P7, P11) correctly identified the activity support system as a source of disturbances when it displays information to support an activity. However, most participants speculated about further potential disturbances and mentioned that the TV might be switched on automatically (4), incoming calls (4), and incoming messages (3). P28 ironically stated: “Friends could write me a message every time when I’m sitting around… Then I would not have any peace when I want to be left alone.” Also the noise of the fan in the smart board was mentioned as a disturbance by three participants.

**Task 4D** In the final task, participants were asked about their strategies to disable all further potential disturbances. All participants of group A solved this task correctly. However, only half of them efficiently disabled both disturbance categories in the PriVis app. The other half disabled every disturbance individually. While this strategy was not as efficient as disabling both categories, it allowed for more informed and fine-grained privacy decisions. Thus, two participants did not disable the automatic door system in order to not lock out their roommates: “I rather do not disable the door system because this would not be very kind for my roommates” (P19). “I don’t touch the door
opening. My roommates might still require it” (P9). One participant (P30) disabled the complete category automations & noise and thus the door system as well, but not the category notifications & interactions and stated: “Now, my roommates cannot come in anymore. I could also disable notifications & interactions. But I rather leave it like that because then my roommates can at least contact me if they want to enter. Furthermore, I still want be warned about a critical health state.” These strategies show that the PriVis app can effectively support users’ privacy decisions by communicating the purpose of existing privacy implications as well as the consequences of control decisions. The fine-grained control options were also positively commented on by P19: “It is useful how accurately I can enable or disable permissions.”

While five participants of group B and C correctly disabled the activity recognition system via its touch display, most other control strategies have only been theoretically mentioned. Most (7) stated that they would pull out the power plugs of the systems, would switch off their smartphones (6) and the wrist band (6), and would set their phones to silent mode. While the door system was not mentioned by most participants of these groups, three stated that they have no possibility to control it, e.g.: “Roommates can always come home. I cannot prevent this” (P4). “I cannot disable the door opening system” (P18). Five participants again expressed their desire for an app that would enable them to control all systems, e.g.: “An app for configuring all of this would be very useful!” (P28). “I would require an app for the smart apartment” (P17). One participant (P26) also stated that controlling all systems would be too bothersome: “I would go in my room, because I would be too lazy to switch it all off!”

Perceived usability, privacy awareness & control of the PriVis app

The usability of the PriVis app is confirmed by the positive results of the ASQ, PSSUQ, and of the scales for privacy tools based on Spiekermann [614], which are depicted in Figures 9.35 and 9.36, respectively.
In the following discussion, we focus on the results of group A and B, which have been supported by the PriVis app. Thus, with all participants we refer to participants of group A and B if not stated otherwise.

For each scale we run two Mann-Whitney U tests to identify significant effects of the group (version of the PriVis app) and gender. While for most scales we did not find significant group-specific differences, we found that the ASQ after the final scenario part was rated significantly higher by participants of group A compared to group B ($U=79.5, p<.05, r=.50$). This shows that participants with the full functional PriVis app were better supported in solving the control tasks after the final scenario part, especially in task 4d in which participants of group B and C were not supported with obvious control mechanisms. Interestingly, however, the perceived control of the PriVis app differed not significantly between group A and B, which suggests that the PriVis app can increase perceived control even if it does not provide direct control.

Furthermore, we found significant gender-specific differences for five scales. Male participants provided higher ratings than female participants for the ASQ after the second scenario part ($U=85, p<.01, r=.60$), the overall ($U=80, p<.05, r=.50$) and SysUse ($U=76, p<.05, r=.44$) scales of the PSSUQ, for the perceived usefulness ($U=82, p<.05, r=.55$), and for the behavioral intention to use ($U=85, p<.01, r=.60$). One reason for these results might be the gender-specific differences in participants’ reported technical affinity (see Section 9.5.3). Indeed we found significant correlations based on Pearson’s $r$ between participants’ technical affinity and the ASQ of part 2 ($r=.70, p<.001$), the overall PSSUQ scale ($r=.54, p<.01$), the SysUse PSSUQ scale ($r=.52, p<.05$), and the behavioral intention to use ($r=.54, p<.01$).

The results suggest that the PriVis app still requires some level of technical expertise in order to be efficiently and willingly used by participants. This has also been confirmed in the qualitative feedback of
ten participants who stated that the PriVis requires some time to become familiar with its features. However, all of them were confident that they would learn it quickly, e.g.: “This is cool. I think I would understand it quickly” (P8). “The PriVis app requires some training, because it provides much information. However, I find all of this information very useful” (P19). Two participants (P17, P22) also stated that the PriVis app would not be suited for elderly users, which aligns with our findings of one of our preliminary user studies (see Section 9.3.3).

Three participants stated that the app provided too many views and information, which was perceived confusing. Five participants further found the long and short touch of a cell confusing, which opened the information pop-up and control dialog, respectively.

However, most (15) participants expressed their acceptance of the PriVis app, which reflects the positive usability results, e.g.: “That’s really great, because I’m concerned about my privacy and here I can configure it like I prefer it right now” (P14). “It makes sense and provides a good overview. This is usually not clear otherwise” (P16). “It’s logically structured and interesting to see where the data is flowing to” (P25). One participant (P19) already tried other user interfaces for configuring privacy preferences and app permissions on Android (see Section 8.2.5 and 9.1). He stated: “For long it is missing something usable to configure what happens. If the PriVis app would work like this, it is clearly the most usable interface I have seen so far.”

In the final interviews we further investigated some of the design features of the PriVis app. All participants liked the distinction of entities in the three zones (personal, ambient, and remote) and also the color coding of green, orange, and red. “The color codes allow for an easy distinction” (P19). “The traffic light metaphor is good. Red is critical because it’s remote” (P29). “Especially the external stuff that tracks you is what one is interested in. Because often you can’t control it” (P4).

However, some (5) participants also expressed concerns about the ambient environment zone: “The zones are cool, but I guess the orange zone would be quite empty” (P1). “Systems in the ambient environment are rather rare because there are not so many smart apartments today” (P29). This position was likely caused by participants’ misconception of the intended scope of the privacy agent. Three participants thought that the PriVis app is limited to the systems they experienced in the scenario even though the purpose of the PriVis app has been clearly communicated in the introduction. Two participants were further concerned about the separation of the ambient and remote zone: “The second and third category are not clearly distinguishable to me” (P8). “Sometimes it was hard to distinguish the orange and red zone. How large is the physical space of the ambient environment?” (P14) This concern points out an interesting question. While the physical territory of a user was defined as the set of all entities at the user’s current location, it indeed might not be clear for users how the current location is defined.
For indoor scenarios this could be a relative position such as a room (as in our study) or a building. For outdoor scenarios it could be an absolute position or defined area. However, the user should be aware of the current scope of the ambient environment, which could be indicated in the pop-up dialog of the zone button or with a hint on the zone button itself. A further extension of the interface could enable users to define the scope of the ambient environment themselves.

All participants further liked the visualization of active and inactive entities as well as the idea of combining observations and disturbances in one privacy interface: “That’s great, because then I can disable both for WhatsApp for instance. I mean notifications and that someone receives information from me” (P9). “I think these are two concepts. But through their visualization as information flows it makes sense” (P2). “It fits well, because both is information flow: something reaches me and something is forwarded from me” (P19). “First, I was kind of confused because this does not exist somewhere else. But it is always data that flows. It’s rare to hear the term disturbance but I like that the app is respecting this” (P13).

Also the visualization of conditions and purpose was a well accepted feature by all participants: “Both info is very useful” (P30). “The purpose is very important to me. I want to know why. It should be beneficial for me” (P22). “Especially the condition is important to me. I want to know when it happens” (P20).

We further asked participants whether they would like to be notified when privacy implications change. While almost all (19) wanted to receive such notifications, only two of them (P13, P14) wanted to be notified about all changes. The majority (17) would accept this feature only if it is configurable in order to receive only notifications about relevant changes: “I only want that when data is being forwarded or if I can decide what I’m interested in” (P19). “I only want to receive notifications on significant changes or when something is forwarded to remote services or persons. Otherwise it would be disturbing” (P10). “For instance, I want to receive a notification only when something is flowing from green to orange or red” (P25). One participant (P20) stated to prefer notifications with summaries of changed privacy implications: “I would prefer if the app collects events first, and then sends a notification with a summary every once in a while. A history would be nice as well” (P20). While the history view is already a part of the privacy agent, it has been excluded from the PriVis app for the study in order to provide users only with the required features. In a future version of the PriVis app the history view could be complemented by a configurable notification feature.

**Perceived usefulness & intention to use the PriVis app**

As shown in Figure 9.36, the perceived usefulness of the PriVis app and the behavioral intention to use it received positive ratings (above neutral) by most participants. Most negative ratings were given by female participants as discussed in the previous section. In the final
interviews, four female participants stated that they would rather not use the PriVis app in everyday situations because: “I don’t really care about it” (P27, group B). “I don’t own such systems or apps” (P30, group A). “I miss the option to control things” (P23, group B). One participant did not provide a reason. However, as also discussed with the results of the task completion time, participants of group B often expressed their desire for a control option: “It would be nice if I would have a block option” (P13). “Too bad that there is no control option. I would use the app more likely if I could switch things off” (P15). These results suggest that the acceptance of the PriVis app is higher with the integrated control option, which is also reflected by the slightly higher median ratings of perceived usefulness and behavioral intention to use of group A compared to group B (see Figure 9.36).

Of the 16 participants who stated to likely use the PriVis app in everyday situations, most stated that they would use it to inform themselves about privacy implications of apps (7), for controlling apps (5), or whenever they do not want to be disturbed (5). Other situations mentioned by participants were at home before going to sleep (P10, P19), at work to concentrate on a task or in a meeting (P19, P20), to block any access to the own location (P14, P29), in shopping malls to learn about present tracking technologies (P4), at public places to learn about video cameras (P10), or whenever something irritating is happening (P14). P1 stated: “I would first use the PriVis app to get an overview and then deny everything I don’t want. Or when I want to change some settings, for example a do-not-disturb setting.” Similar, P13 stated: “First, I would inform myself and then allow only important disturbances. For example, I always set my phone to silent mode and my girlfriend always is gonna killing me because I never pick up the phone when she is calling.”

In the final interviews, we also asked participants of group C about their attitudes towards an application that would visualize the flow and access of their personal information and of potential disturbances. However, we did not provide any details about how such an interface could look like. All of them liked the idea of such an application to visualize their information flows: “This would be really useful. I want to know that!” (P11) “It would be very helpful if I could see with whom I share information with. But control would also be important” (P12). “It would be really cool to have an app that shows everything that has access. It would be even cooler if the app would allow to figure out how to disable such things, because this is often not obvious” (P26). “This would be nice. Then I would have more control” (P21). The feedback also highlights that control is desired by participants and awareness alone might not be sufficient for the acceptance of such an application.

Also the idea of visualizing potential disturbances was accepted by most (6) participants of group C: “I would use it in my shared apartment” (P2). “This would be an interesting option. For instance, in a connected home this would be very useful” (P7). “This would be nice. Then I
could adapt myself to the situation” (P21). “I would like this, because I want to configure the things on my own. For example if my smartphone suddenly starts to vibrate” (P11). However, four participants stated to rather not use this feature: “At home I can control everything on my own” (P3). “I would not need it because I would switch everything off on my own. You further cannot exclude all disturbances, for example neighbors. Such an app would be more of a gimmick” (P26). “If I could configure the cleaning robot I would not need it” (P28).

Finally, we asked participants of group C whether such an app could increase their acceptance of technology similar to those experienced in the scenario. While two participants did not expect an app to increase their acceptance, most (8) participants agreed that it likely would increase their acceptance: “Absolutely. Then my mistrust would be gone. This would make things easier” (P21). “If the app would be reliable and would provide trustworthy information. Otherwise I would be skeptical if everything is true and legally valid what the app is telling me” (P26). “I would think so if it is controllable” (P7). “I guess yes, because then one will understand its benefits. However, I want to have control” (P12). “If I could see it, then I could make more informed decisions about what I want to use. Control would be even better. Then I would probably have no negative attitudes towards technology” (P24). These results suggest that the PriVis app might increase users’ acceptance of technology, especially when it enables users to control existing privacy implications. We discuss the investigation of this question in the following section.

Privacy concerns and technology acceptance

We measured participants’ acceptance of the experienced technologies with four items of perceived usefulness (PU) based on Davis et al. [180] and four items of behavioral intention to use (BIU) based on Mick and Fournier [454]. We further measured participants’ perceived privacy concerns (PPCrsns), perceived privacy awareness (PPA), and perceived privacy control (PPCtrl) with respect to the experienced technologies. These factors have been measured with 14 items based on Spiekermann [614]. The scales have been adjusted in order to reflect also disturbances. All items were rated on a 5-point Likert scale. We conducted a confirmatory factor analysis in order to eliminate items with unsatisfying factor loadings. The analysis resulted in the elimination of two items from PU, two items from the BIU, three items from the PPCtrl, and two items from the PPCrsns.

The results of the perceived privacy concerns are depicted in Figure 9.37. It shows that for most technologies participants expressed high privacy concerns (above neutral), with exception of the cleaning robot. We could not find any effects of the group on the perceived privacy concerns. High privacy concerns among groups have also been reflected in numerous qualitative feedback of participants during the scenario and in the final interviews: “This all has some surveillance char-
actor and low benefit. Maybe the Roomba would be ok” (P2). “That’s all affecting my privacy. I would rather not get those things” (P3). “This is a risk for my privacy. If I would not need those things, I wouldn’t take the risk” (P28). “For me everything was negative and scary, especially the door system” (P29). Privacy concerns regarding the automatic door system were primarily caused by its presence sharing feature: “I would not want that it tells someone when I come home” (P22). “I disliked that it shared my presence” (P12,P15).

The activity support system and the fitness app received the most negative feedback, which aligns with the perceived privacy concerns shown in Figure 9.37. As expected, the fitness app was mostly criticized for its live-sharing feature: “I wouldn’t use this app. No one should know what I’m doing.” (P14) “I would rather not use the app, especially not the sharing-with-friends feature!” (P30) “It would be worrisome if friends would know that I’m sitting. This wouldn’t be worth it” (P16). “The message from Mike was very scary. This was a frightening scenario” (P15). “That’s really creepy [...] creepy Facebook sharing app!” (P15) “I didn’t like that Mike knew my activity. Sometimes I just want to be unobserved” (P11).

Most privacy concerns regarding the activity support system were caused by its video camera in the living room: “The camera makes me nervous [...] I would feel disturbed. It’s like the Xbox: I don’t have a clue who is observing me” (P9). “I would always feel observed by the camera. I want to be unwatched at home” (P11). “It’s critical and reminds my of the NSA and Big Brother” (P26). “I do not want to be filmed all the time” (P10). “The camera is creepy even though it is only local” (P20). “I don’t want a camera even if it is only for this purpose” (P15). The results show that a video camera is perceived as very intrusive no matter what the purpose of the camera is. This aligns with the results of previous studies, which we have discussed in Chapter 4.4.

The high privacy concerns about the activity support system are also reflected in the negative results of participants’ perceived privacy awareness and control of the system, as depicted in Figure 9.38 and Figure 9.39, respectively. Based on the calculation of Pearson’s ρ we found significant negative correlations between participants’ perceived privacy concerns and their perceived privacy awareness (ρ=.38,
p<.001) as well as between their perceived privacy concerns and their perceived privacy control (r=.67, p<.001). While we cannot directly derive a causality from the data, a likely model is that an increase in perceived awareness and control of privacy implications can decrease users’ perceived privacy concerns.

In order to find group-specific differences of participants’ perceived privacy awareness and control, we ran a Kruskal Wallis test for each system. We found a significant effect of the group for the perceived privacy awareness of the health app (H(2)=6.85, p<.05), automatic door system (H(2)=10.79, p<.01), and fitness app (H(2)=8.77, p<.05). Post-hoc Mann-Whitney tests with Bonferroni correction showed that participants’ perceived privacy awareness in group B was significantly higher than those of participants in group C for the health app (p<.05, r=.53), the automatic door system (p<.01, r=.63), and the fitness app (p<.05, r=.49). In group A, participants’ perceived privacy awareness was significantly higher than in group C only for the automatic door system (p<.01, r=.63). However, even though we did not find significant differences for all systems, participants’ perceived privacy awareness shows higher tendencies in group A and B compared to group C for all systems with exception of the cleaning robot (see Figure 9.38). Thus, we accept our hypothesis H3, that the privacy agent increases perceived privacy awareness.
While the perceived privacy control also shows higher tendencies for participants supported by the PriVis app (except for the cleaning robot), we found significant differences only for the health app ($H(2)=6.23$, $p<.05$). Here, participants that were not supported by the PriVis app perceived significantly lower privacy control than participants of group A ($p<.01$, $r=.58$) and of group B ($p<.05$, $r=.54$). A possible reason for this result might be the effect of the introduction in which participants of group A and B were introduced to the PriVis app with many examples of how to control privacy implications of the health app. While in the other parts of the scenario, control tasks were mostly limited to the control of disturbances. However, when we looked only at male participants we further found a significant effect of the group for perceived privacy control of the automatic door system ($H(2)=7.15$, $p<.05$). Here male participants of group A perceived significantly higher privacy control than male participants of group C ($p<.01$, $r=.61$). Thus, we partially accept our hypothesis $H_4$ that the privacy agent increases perceived privacy control.

We found similar results for the perceived usefulness of the systems, see Figure 9.40. A significant effect of the group was found for the fitness app ($H(2)=6.19$, $p<.05$) and, when considering only male participants, for the automatic door system ($H(2)=5.45$, $p<.05$). Post-hoc Mann-Whitney tests with Bonferroni correction showed that par-
Table 9.2: Spearman’s $\rho$ correlations between perceived privacy concerns (PPCrns), perceived privacy awareness (PPA), perceived privacy control (PPCtrl), perceived usefulness (PU), and behavioral intention to use (BIU). The significance level for all correlations is $p < .001$.

<table>
<thead>
<tr>
<th></th>
<th>PPCrns</th>
<th>PPA</th>
<th>PPCtrl</th>
<th>PU</th>
<th>BIU</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPCrns</td>
<td>- -38</td>
<td>- -67</td>
<td>- -51</td>
<td>- -42</td>
<td></td>
</tr>
<tr>
<td>PPA</td>
<td>- -38</td>
<td>- -48</td>
<td>- -41</td>
<td>- -44</td>
<td></td>
</tr>
<tr>
<td>PPCtrl</td>
<td>- -67</td>
<td>- -41</td>
<td>- -47</td>
<td>- -56</td>
<td></td>
</tr>
<tr>
<td>PU</td>
<td>- -51</td>
<td>- -41</td>
<td>- -47</td>
<td>- -77</td>
<td></td>
</tr>
<tr>
<td>BIU</td>
<td>- -42</td>
<td>- -44</td>
<td>- -56</td>
<td>- -77</td>
<td></td>
</tr>
</tbody>
</table>

Participants of group A perceived the usefulness of the fitness app significantly higher than participants of group C ($p < .05$, $\rho = .50$). Further, when respecting only male participants, the perceived usefulness of the automatic door system was also significantly higher in group A than in group C ($p < .05$, $\rho = .48$). Thus, at least for the automatic door system, male participants of group A perceived significantly higher privacy awareness, control, and usefulness than participants of group C. This result is also supported by the significant correlations (Spearman’s $\rho$) of participants’ perceived usefulness with perceived privacy concerns ($\rho = -.51$, $p < .001$), perceived awareness ($\rho = -.41$, $p < .001$), and with perceived control ($\rho = -.47$, $p < .001$), see Table 9.2.

For the behavioral intention to use (see Figure 9.41), we only found an effect of the group for male participants regarding the fitness app ($H(2) = 6.193$, $p < .05$). In group C, male participants’ behavioral intention to use the fitness app was significantly lower compared to male participants of group A ($p < .05$, $\rho = .45$) and to male participants of group B ($p < .05$, $\rho = .50$). This result is also supported by the significant correlations of participants’ behavioral intention to use with perceived privacy concerns ($\rho = -.42$, $p < .001$), perceived awareness ($\rho = -.44$, $p < .001$), and with perceived control ($\rho = -.56$, $p < .001$), see Table 9.2. Thus, at least for the automatic door system and the fitness app we can accept our hypothesis $H_5$ that the privacy agent can potentially increase users’ acceptance of the technology.

One reason why we found some group-specific differences only for male participants, is the significant gender-specific difference of participants’ perceived usefulness and behavioral intention to use in group C for the automatic door system (see Figures 9.40 and 9.41). Female participants in group C expressed a significantly higher ($p < .05$) acceptance of the system than male participants in group C. Another reason might be that the perceived usability of the PriVis app was slightly higher for male participants who also expressed a higher willingness to use the PriVis app. This in turn might be caused by their higher technical affinity reported in the online survey. However,
this effect might become less obvious when users become more familiar with the user interface. In order to investigate this question, the PriVis app could be evaluated in a real-world setting over several days or weeks.

For the health app, the activity support system, and the cleaning robot, we could not find any significant group-specific differences in participants’ perceived usefulness and behavioral intention to use. For the activity support system, this is likely due to the very high privacy concerns caused by the camera. In contrast, for the cleaning robot, this is likely caused by its few associated privacy concerns and its general usefulness, which was reflected in several comments of participants: “The Roomba is awesome!” (P19) “I like it. I could save money” (P12). “It is very nice that the cleaning robot reacts to the electricity rates” (P11). Finally, for the health app, this might be caused by the fact that the perceived privacy awareness of participants in group C was relatively high due to the detailed introduction of the health app in the first part of the scenario. Furthermore, the general usefulness of the health app was perceived as very useful as also reflected in participants’ feedback: “The health app is useful for elderly people” (P14,P16,P22,P23,P26). I would suggest this to my parents (P21). “I would use the health app if I would have serious health issues” (P9). Thus, even though the health app was perceived as useful the behavioral intention to use was much lower because participants did not consider themselves as the target group.

**Understanding of privacy**

As a final question of the post study interview, participants were asked about their understanding of the term privacy. As expected, the notion of information privacy as one’s control of access to personal information was the most prevalent understanding of privacy and was mentioned by 17 participants. Seven participants mentioned self-determination as the most important aspect of privacy and eight participants stated to require a place of solitude and peace to have privacy, e.g.: “Privacy is when I have peace and quiet and cannot be disturbed” (P25). “For me it is self determination and being free from disturbances” (P11). “Privacy, for me, is the ability to decide at home if anyone can disturb me from the outside. It is also about controlling technology” (P28).

We further asked participants whether they consider disturbances as a factor of privacy. Six participants stated that this rather is a different concept, e.g.: “I don’t think so. Even if it is silent, someone can access my personal information” (P21). “Rather not. Disturbances are disturbances” (P10). “It is maybe a connected concept but privacy is more about being unobserved. Noise would not disturb my privacy” (P30). “It is rather something different. However, it is very important to me” (P27).

For the remaining 24 participants it clearly was considered a part of privacy, e.g.: “Yes, absolutely. You need to be able to control disturbances in
order to have privacy” (P5). “Of course. When I’m at home I want to have my peace” (P17). “I think so, because something is intruding my privacy then” (P7). Three participants stated that it depends on the current location: “At home yes and maybe in the office but not in public” (P19). “It depends where you are. You don’t have the right to be undisturbed at a public place. However, you have at home” (P13). The last statements confirm our concept of environment types with different expectations of privacy awareness and control from private to public environments, which have been discussed in Section 5.1.

While we are aware that participants’ answers to the last questions might have been influenced by the study setup and involved technologies of the scenario, they yet provide valuable indicators of the appropriateness of our concept of territorial privacy.

9.5.5 Discussion

The evaluation of our final user interface confirmed its usability and showed that participants were effectively supported with awareness and control of involved privacy implications. Most tasks have been correctly solved by participants supported by the PriVis app. Furthermore, they required less or the same time to correctly complete a task as participants without support who often were not able to solve a task correctly. One reason for this was that the common approach to present privacy policies in textual form was perceived as too cumbersome and participants were not willing to spend time reading them. This result aligns with findings of other studies regarding privacy policies of websites [328, 329, 30]. Another reason was that the activity support system was overlooked by most participants even though it was prominently placed in the room and provided information on its screen. While this fact caused most participants of group C to fail in the tasks in which the activity support system was involved, participants of group A and B were effectively made aware of the system by the PriVis app and thus were able to correctly solve these tasks. This highlights the effectiveness of the PriVis app especially in situations in which systems are invisibly embedded in the environment. A reason why the activity support system was overlooked by so many participants might be the artificial atmosphere of the lab study. However, several participants confirmed their good immersion in the scenario, e.g.: “This was a very realistic study. I could imagine all the systems very well” (P7). “It was an interesting study setup and very realistic despite some limitations (e.g., no real apartment)” (P28).

An interesting finding was the control strategy of some participants from group A in the final task 4d. While participants were asked to prevent all further disturbances, three participants chose to make more fine-grained control decisions. They recognized that they might lock out their roommates when they disable all “automations & noise”
or that they won’t be warned about a critical health state anymore when they disable all “notifications & interactions”. Thus, they only disabled unimportant disturbances or those with acceptable consequences. This shows that the PriVis app can effectively support users’ privacy decisions by communicating the purpose of existing privacy implications as well as the consequences of their control decisions.

The integration of territorial privacy aspects in the PriVis app was highly accepted by participants. They liked the idea of visualizing observations and disturbances as information flows in a single user interface, which could serve as a central tool for privacy awareness and control. Also, the territorial separation of entities in the personal, ambient, and remote zones was supported by participants. However, some participants were concerned about the usefulness of the ambient zone with a low number of smart technologies in our today’s environment. Furthermore, one participant was confused about the boundaries and size of the ambient zone, which is a valuable hint for the optimization of the user interface. While the boundaries of the ambient zone (i.e., the physical territory) can be defined at different levels (e.g., as a room, a building, or a public place), users should be aware of its current scope. A valuable extension to the user interface could be the user-defined scope of the ambient zone, which then must be respected in the territorial privacy model.

In general, the acceptance of the PriVis app (in both versions) was very high, which has also been confirmed by many positive statements in the post-study interviews. Thus, the missing control feature of the app version in group B did not significantly influence its acceptance even though participants of group B expressed their desire for a control option in the user interface. However, we found that the acceptance was significantly higher for male participants. Because we did not find any gender-specific differences in participants’ general privacy concerns, one reason for the difference in acceptance might be the higher technical affinity of male participants. This might have allowed them to more quickly understand the features of the interface, which was reported to require some initial familiarization by several participants. However, most participants were optimistic to become familiar with all app features after using it for one day. Thus, it might be interesting to evaluate the acceptance of the PriVis app in a long-term study in which participants have more time to familiarize themselves with the different features of the PriVis app.

Participants’ privacy concerns towards the experienced technologies were fairly high and were not significantly different between groups. However, we found that the PriVis app could significantly increase participants’ perceived privacy awareness and control of some of these technologies. The effect of the PriVis app on the perceived privacy control was further found to be higher for male participants, which also might be influenced by their higher technical affinity.
Significant effects of the group on the acceptance of a technology have been found only for the automatic door system and the fitness app. However, the effect again was higher for male participants. Thus, while the PriVis app could potentially increase users’ acceptance, the effect should also be investigated in a long-term study in which we can assume that participants are familiar with the PriVis app.

**Study limitations**

There is a number of limitations of our study, which must be considered when interpreting the results. As a first limitation the study was conducted in a seminar room of our institute due to budget constraints and the lack of a smart living lab at our campus. However, even though the study did not provide an authentic real-world smart apartment, the experienced systems were implemented as full functional prototypes and some participants confirmed the realistic nature of our setup.

Another limitation is the sample size of ten participants per group. While we assured the homogeneity of groups in terms of age, gender, technical affinity, and general privacy concerns, our results might not be transferable to the general population. Furthermore, all participants were German and thus the results might be influenced by cultural norms. Nevertheless, our results provide valuable insights for the design and effectiveness of privacy tools supporting awareness and control in UbiComp.

Finally, not all features of the PriVis app have been evaluated as part of this study. The utility of the history view and of the privacy profile view could best be evaluated as part of a long-term study in which also the effect of the familiarization with the PriVis app can be better investigated.

**9.5.6 Design implications**

The results of our evaluation provide several design implications for the development of privacy-friendly UbiComp applications as well as for the development of a user-centric privacy interface.

An interesting insight of our study was that most participants were not aware of the activity support system and the active video camera even though both systems were visibly placed in the environment. Furthermore, both systems indicated their active state. The activity support system presented an explicit notice on its display and the camera was equipped with a red light. Thus, even though both systems were not invisibly embedded in the environment and provided explicit notices, most participants were not aware of their presence. This highlights that system designers of UbiComp applications should not rely only on physical awareness indicators and should instead complement them by supporting centralized awareness so-
olutions as proposed by our framework. This would enable users to be aware of such systems and also of invisible UbiComp systems as demonstrated by the results of our PriVis app evaluation.

Similar to related work [328, 329, 30], we found that the common textual presentation of privacy policies requires too much effort to gain awareness of privacy implications. Most participants were not willing to read them in our study. This further motivates that system designers of UbiComp applications should support centralized awareness solutions that are able to provide user-friendly presentations of privacy implications as proposed by our PriVis app.

Further, we found that participants’ reactions towards a system were especially negative when they saw no benefit in the features of the system or when they were not aware of the purpose of specific features. This aligns with the findings of related work discussed in Chapter 4. The results suggest that system designers of UbiComp applications should clearly state the benefits and purposes of system features, in particular of features that affect users’ privacy. While the PriVis app was able to communicate the purpose of such features to users, the purpose description in some cases was perceived as too vague. For instance, the activity support system provided the purpose description *activity support for an information disturbance channel*, which refers to the system’s feature of presenting activity supporting information on the ambient display. Three participants stated that it remained unclear how their activity would be supported. Thus, purpose descriptions in channel policies should be specific and provide user-friendly explanations with appropriate details.

Our study has further shown that being aware of a purpose supports privacy decision making. In the control task of disturbances, three participants chose to make more fine-grained control decisions as required for task solving, because they respected the consequences of their control decisions for specific purposes presented by the PriVis app. This highlights that a user-friendly presentation of purposes and their dependencies as proposed by our PriVis app can reduce the need of making users explicitly aware of consequences of their control decisions. Thus, presenting dependencies of purposes and privacy implications should be respected when designing user-centered privacy interfaces.

According to our concept of territories and boundaries discussed in Section 5.2, the separation of entities by three territorial zones was appreciated by participants. The separation enables users to be aware of personal and physical border crossings. As expected, we found that physical border crossings were perceived as most relevant by participants. Participants also expressed the desire of being notified when such border crossings occur. Thus, designers of user-centered privacy interfaces should especially focus on making users aware of such physical border crossings. While notifications are a reasonable
9.6 Summary

In order to support users with privacy awareness and control of UbiComp technologies, we developed a graphical user interface in an iterative design process. The user interface is an integral part of the privacy agent and maps the instantiated territorial privacy model of the privacy engine onto the user level. Privacy awareness is supported by different views to visualize current and past privacy implications. These views further allow users to exert direct privacy control decisions. Indirect privacy control is supported by a privacy profile view, which allows users to specify individual privacy preferences.

The final prototype of the user interface (the PriVis app) has been implemented as an Android application for smartphones and has been evaluated in a realistic scenario-driven lab study with functional prototypes of different UbiComp technologies. The results of our evaluation show the acceptance of our territorial privacy concepts and confirm the usability and effectiveness of our user-centered privacy management approach.
SUMMARY

The primary vision of Ubiquitous Computing (UbiComp) is to enhance our everyday lives by smart and unobtrusive technology (as discussed in Section 2.1). Since Weiser’s initial formulation of this vision in 1991, many UbiComp applications have emerged, ranging from smart environments, to mobile and wearable applications, to applications in healthcare and assisted living (see Section 2.3). While many of these applications are still part of ongoing research efforts, we already see several technological trends towards UbiComp today, e.g., the increasing popularity of wearable fitness devices and smart watches (see Section 2.4).

Although UbiComp applications promise to make our lives easier, smarter, or just more comfortable, they also pose new risks for our privacy (see Section 3.4). The smartness and context-awareness of UbiComp often relies on the collection of personal information and its communication to several other entities. Furthermore, UbiComp systems often autonomously initiate interactions with users or autonomously intervene in their environments. Those UbiComp characteristics (see Section 2.2) could cause undesired observations and disturbances and thus could affect users’ territorial privacy. While most existing research focuses on aspects of information privacy, we define our concept of territorial privacy to cover both aspects of informational privacy and aspects of physical privacy, which refers to the invasion of personal space and to disturbances in the physical world as discussed in Section 3.2.

In this thesis, we investigated the issue of privacy in UbiComp by developing a user-centered framework for privacy awareness and control, which is based on the concept of territorial privacy. We summarize the main contributions of this work in the next section, followed by a discussion of future research directions.

10.1 CONTRIBUTIONS

As a motivation for our privacy framework we identified the main privacy implications of UbiComp systems and conducted two studies in which we investigated the privacy implications of zero configuration networking (Section 3.4.2) and mobile messaging applications (Section 3.4.3). Both technologies are commonly used on mobile devices today. Our results show that those prevalent technologies pose several privacy implications, which users are often not aware of. Together with similar findings of related work, our results motivate the need of en-
hancing privacy awareness in UbiComp and contribute to the identification of the main privacy implications stemming from UbiComp systems (research question R1.1, see Section 1.2).

In order to guide the development of our territorial privacy model, we conducted an extensive literature review of existing user studies that investigated the aspects of privacy implications users want to be aware of and want to control (R2.1), see Chapter 4. We identified essential factors that influence awareness and control of privacy-affecting observations and disturbances at the user level. These factors were considered in the design of our territorial privacy model in order to support awareness and control of who affects privacy, how it is affected, and why it is affected (see Figure 4.3). We complemented the results of the literature review with further research by conducting an online survey (see Section 4.6) and a focus group session (see Section 4.7) in which we investigated privacy concerns of elderly persons towards ambient-assisted living technologies. Such assisted living technologies are one of the major UbiComp applications envisioned. However, elderly persons will likely be the most challenged in coping with such technological changes, especially in terms of privacy awareness and control. Our results confirmed the relevance of our identified factors for providing awareness and control of privacy-affecting observations and disturbances in UbiComp.

Based on the results of the literature review and our definition of territorial privacy, we developed a graph-based territorial privacy model in Chapter 6, which addresses informational and physical privacy aspects (R1). The territorial privacy model allows to capture which entities affect a user’s privacy, how and why. According to our territorial privacy concept, the aspect of how privacy may be affected further respects observations and disturbances and thus extends the common limitation to information privacy of most related work on UbiComp privacy. The features of our model support privacy awareness and control (R1.3). That is, the model allows to infer dependencies between entities and consequences or conflicts of potential control decisions. Our model further supports identification of the most efficient control strategies, which enables enforcement of users’ privacy decisions at the system level. We demonstrated the feasibility of our model by applying it to three representative UbiComp use cases (see Section 5.5), which take place in different environment types ranging from private to public.

In order to enable the instantiation of the territorial privacy model at the system level (R2.1), we developed channel policies as a container format for the specification and discovery of an entity’s privacy implications (see Section 7.3). Channel policies provide detailed information about an entity as well as how and why this entity is affecting a user’s privacy with respective observations and disturbances.
Furthermore, channel policies provide references to available control points for privacy enforcement.

We developed five discovery and enforcement modules (see Chapter 8) to enable the discovery of such channel policies (R2.2) in actual UbiComp systems and the enforcement of users’ privacy control decisions (R2.3), respectively. To cope with the heterogeneity of UbiComp systems, with their different privacy implications, and with the different settings and conditions of a user’s environment, different discovery and enforcement mechanisms have been developed. The modules implement both optimistic and pessimistic approaches, in order to satisfy the different requirements and assumptions.

The personal device module (see Section 8.2) allows to discover and control privacy implications of personal devices (e.g., of a smartphone or a wearable device). It incorporates both an optimistic and pessimistic approach for privacy awareness and control. The pessimistic approach provides awareness and control of uncooperative or malicious entities by integrating a privacy enforcement layer in the Android application framework. The optimistic approach is based on the assumption that entities (e.g., mobile applications) provide valid channel policies.

The trusted environment module (see Section 8.3) supports discovery and enforcement in a user’s physical environment (e.g., at home or at work). The module provides an optimistic approach for privacy awareness and control. One part of the module assumes the existence of a trusted infrastructure that allows direct discovery and control in collaboration with individual entities. Further module features assume the existence of a trusted system that allows indirect control through the delegation of privacy enforcement according to a user’s privacy preferences. The implementation and evaluation of the module have been conducted as part of the EU-funded ATRACO project.

In order to support the discovery of privacy implications in public environments we proposed the beacon-based discovery module (see Section 8.4) and community-based discovery module (see Section 8.5). The first module provides an optimistic approach and assumes the collaboration of entities in order to provide reliable broadcasts of PriFi beacons, which contain channel policies in vendor-specific information elements of WiFi beacons. Our implementation of a lightweight prototype showed that entities could easily be equipped with the beaconing approach to communicate their channel policies. In contrast to the beaconing approach, the community-based discovery module provides a pessimistic approach and thus does not require an entity’s collaboration. It assumes that privacy implications are collected by users in a crowd-sourced manner. We demonstrated the feasibility of this approach for the crowd-sourced collection of information about public video cameras via a mobile Android application.
The ability to enforce privacy decisions depends largely on the availability of control points. Therefore, we propose the privacy signaling module (see Section 8.6) as a fallback strategy in situations without direct control. Such situations especially occur in shared or public environments with undesired disturbances stemming from other persons. Our Android-based prototype implementation of the module allows to wirelessly communicate own privacy preferences (e.g., do not disturb) to other entities nearby. Furthermore, it supports the automatic adaptation (e.g., switch to silent mode) according to received privacy preferences of others. The results of our field trial have shown that the signaling approach is accepted and would be potentially useful in several everyday situations.

The proposed discovery and enforcement modules have been evaluated for their technical feasibility and efficiency. The results show that the developed framework is able to efficiently discover and control privacy implications in UbiComp for different scenarios. Most of our modules can be integrated into existing UbiComp applications without requiring major modifications, which highlights the practicability of our approach. Furthermore, our modular approach allows for a practical deployment of only a selection of the proposed discovery and enforcement mechanisms, which makes them re usable for several UbiComp scenarios. Therefore, our framework provides a comprehensive realization of territorial privacy at the system level (R2).

In an iterative design process, we developed a user interface for user-centered privacy management (see Chapter 9). The proposed interface maps an instantiation of the territorial privacy model onto the user level (R3.1). Privacy awareness is supported by different visualization approaches which are able to present complex privacy implications of UbiComp systems (R3.2) at different levels of granularity. The general visualization approach is based on a table view in which privacy-affecting entities are presented in columns and privacy implications in form of observations and disturbances are presented in rows. This approach allows users to be aware of privacy implications of personal, ambient, and remote entities as well as existing dependencies and information flow between those entities. More detailed information such as conditions or the purpose of privacy implications is presented in additional popup dialogs.

Furthermore, users are supported in privacy decision making and in controlling systems according to their privacy needs (R3.3) with direct control options and by the specification of privacy preferences. Direct control options are integrated in the table view and allow users to deny specific entities, privacy implications, or purposes of privacy-affecting observations and disturbances. Privacy preferences can be specified via a separate privacy profile view in which users can create profiles with context-based rules for specific situations.
We evaluated our proposed user interface in a scenario-driven user study with several functional prototypes of typical UbiComp systems causing complex privacy implications in form of different observations and disturbances. The results suggest that our territorial privacy concept and our approach to support privacy awareness and control are highly accepted. The results further show that the developed user interface can **effectively support users with privacy awareness and control of complex privacy implications in UbiComp (R3)**.

**10.2 Outlook**

Our evaluations have demonstrated the feasibility of our proposed framework for user-centered privacy awareness and control in UbiComp. Furthermore, our final user study confirmed that the territorial privacy concept and its associated model at the system level could be successfully mapped onto the user level in order to effectively enhance users’ privacy awareness and control. However, there are still some challenges for future work.

One aspect is the knowledge base of privacy implications, which is represented in our proposed territorial privacy model. While this knowledge base is currently based on the discovery of channel policies, it could be extended by creating heuristic models of privacy implications based on previous graph instantiations. This would allow to also model uncertain privacy implications of entities that do not provide channel policies or provide only channel policies with incomplete information. Such an approach could be utilized to learn from virtual or logical sensors, which refers to entities that infer new observation channels from one or more incoming channels. For instance, if we know that an entity infers a user’s activity from the combination of an acceleration observation channel and a heart rate observation channel, we could model this as a potential privacy implication for other entities that have access to similar observation channels.

Previous graph instantiations could likewise be analyzed for common or recurring arrangements of observation and disturbance channels. For instance, knowing that a specific path of observation channels always triggers the same disturbance channel would enable to model missing parts of the path with some uncertainty. The results of those and similar graph analysis approaches could be merged into a central knowledge base, which would support our proposed discovery process in order to model uncertain privacy implications.

Our proposed discovery and enforcement modules apply optimistic as well as pessimistic strategies for the discovery and control of privacy implications. The optimistic control strategies assume the collaboration of privacy-affecting entities. That is, entities must provide valid channel policies and control points. The feasibility and success of these strategies to some extent depends on the support by appro-
priate legal frameworks and regulations. The European Union’s current investigations [219, 220] of reforming their data protection rules pose a relevant step in the right direction as they foster important privacy practices such as the right to be forgotten, easier access to own data, or privacy by design. In the US, the FTC [244] has recently proposed recommendations and best practices for privacy in a connected world, which emphasize the relevance of the data minimization and the notice and choice principles in the context of UbiComp (see also Section 3.3). Peppet [513] has proposed similar regulations as one of the first legal work addressing privacy issues of the Internet of Things. He argues that there is an urgent need for regulation, because consumers of available smart devices are already exposed to privacy risk: “As time passes it will likely become more difficult, not easier, for consumer advocates, regulators, and legislators to act. The Internet of Things is here. It would be wise to respond as quickly as possible to its inherent challenges” [513].

However, even if such privacy rules and regulations were established, they would have to be mapped onto concrete privacy mechanisms for which currently no standards exist. Such standards should be developed by the collaboration of regulatory authorities, privacy experts, and industrial stakeholders. Otherwise their adoption will likely fail, as shown by the earlier attempts of P3P [169] and do-not-track [443] to enhance privacy awareness and control on websites. The contributions of this work could provide valuable input for future standardization attempts for supporting privacy awareness and control in UbiComp. As our results suggest that providing users with awareness and control of a system’s privacy implications could increase their acceptance of the system, there could also be an economic interest on the part of the industry in contributing to such standards.

Even though our proposed personal device module combines both optimistic and pessimistic strategies, it comes with some limitations. The module can only reliably enforce privacy control for entities residing on a user’s personal devices (e.g., mobile applications). However, as soon as observations and disturbances cross the personal or physical boundary (e.g., when a wearable sensor communicates vital parameters to a remote service), privacy control relies on optimistic strategies. While there are attempts to enforce privacy control based on trusted computing remotely [343], those mechanisms assume that remote entities deploy and integrate specific software components in their system or application logic. However, if this burden would be accepted by stakeholders or even legally enforced, similar approaches could be combined with our optimistic approaches in order to enforce privacy control of remote entities.

Our privacy signaling approach has been proposed as a fallback strategy in situations without direct control, especially in shared or public environments with undesired disturbances stemming from oth-
er persons. While its effectiveness also strongly depends on the widespread deployment of applications that are capable of receiving such privacy signals, it could be supported by the deployment of proxy devices. For instance, public displays in waiting areas or train compartments could summarize dominant preferences of present persons signaling their preferences. Future work could investigate the social acceptance and effectiveness of such approaches in field deployments.

At the user level, we have demonstrated the usability of our user-centered privacy management application, which provides a user interface to an instantiation of the privacy graph. While our results suggest that users are able to efficiently apply the user interface after an initial familiarization phase, the interface might be challenging for users with little or no technical experience, e.g., elderly persons. Future work could investigate the effectiveness of more simplified versions of our user interface or spoken dialog systems as proposed by elderly participants in one of our usability studies. Furthermore, our final evaluation was limited to a predefined scenario conducted in a lab environment. A more longitudinal study of the user interface in everyday situations could provide further insights on its effectiveness, especially for the history view and privacy preference configuration.

The contributions of this work have demonstrated the feasibility of a user-centered approach to provide individuals with awareness and control of privacy implications in UbiComp. Several of our proposed discovery and enforcement mechanisms have been developed in a modular approach and implemented as stand-alone solutions, which makes them reusable and practically deployable in existing UbiComp applications. We believe that our contributions can help shape the design of future UbiComp systems to be not only convenient and supportive but also privacy-friendly.
ACKNOWLEDGMENTS

Writing this thesis was an exciting yet challenging experience, which would not have been possible without the help and support of many other persons. First of all I want to thank Prof. Michael Weber, my supervisor and mentor, for giving me the freedom of conducting my research in any favored direction. I am highly grateful for his support in completing this thesis, as well as in inconvenient situations beyond our professional relationship. I also want to thank my second supervisor Prof. Frank Kargl for inspiring my research interests in security and privacy. He was always a great mentor and provided valuable advice and constructive feedback to several contributions of this thesis. My gratitude further goes to Prof. Sarah Spiekermann who is one of the leading researchers in privacy and ethical computing. I am very honored and thankful that she agreed to be a referee for my thesis at such short notice.

I further want to thank my colleagues Florian Schaub, Stefan Dietzel, Björn Wiedersheim, Thorsten Mahler, Elmar Schoch, and Boto Bako who facilitated the start of my academic journey. I am thankful to have had Björn as my steady office mate who always enabled a productive work climate and was a helpful expert in any hardware issues. We not only shared the same office but also several nice sailing and samba adventures. A deep gratitude goes to my colleague and friend Florian Schaub who supported my work from the very beginning. His expertise and academic ambitions have led to countless discussions that significantly influenced the progress of this thesis. I am also very grateful for his valuable and extensive review. I further want to thank Dennis Ott, Julian Seifert, and Stefan Dietzel for reviewing parts of this thesis. Stefan has also been a good friend since my early days in Ulm.

My time at the Institute of Media Informatics has been always enjoyable and was influenced by many other colleagues and students which I want to thank sincerely. Special thanks go to my colleagues Björn Wiedersheim, Julian Seifert, Christian Winkler, Florian Geiselhart, Jan Gugenheimer, David Dobbelstein, Katja Rogers, Julian Frommel and Marcel Walch for many stress-relieving foosball sessions. I further want to thank all of my other colleagues, namely Prof. Enrico Rukzio, Prof. Timo Ropinski, Frank Honold, Felix Schüssel, Sven Reichel, Naim Asaj, Wesam Herbawi, Jonas Beinder, Julia Greim, Michael Rietzler, Katrin Plaumann, Philipp Hock, Dennis Wolf, Claudia Wainczyk, and Michael Haug for interesting discussions, enjoyable lunch breaks or Weißwurstfrühstücke, and challenging squash games.
I am also grateful to have supervised several talented students whose work supported parts of this thesis. Especially I want to thank Julia Greim, David Herges, Sebastian Thoma, Christoph Bachmaier, David Piendl, Jens Nickels, Dominik Lang, Ewgenji Leibmann, Nelli Natan, and David Thierbach for their good work and collaboration.

Concerning the study about privacy implications of mobile messaging applications, I want to thank Andreas Buchenscheit, Matthias Schneider, and Andreas Neubert for the interesting and enjoyable collaboration on this topic.

The first three years of my research were supported by a fellowship for individual doctoral training funded by the Landesgraduiertenförderung (LGFG) for which I want to express my gratitude.

Furthermore, this thesis would not have been possible without the support and encouragement of my family and friends. A great gratitude goes to my parents Claudia and Johannes Könings as well as to my sister Christine Könings who always supported me on my way to finish this thesis with encouraging words or by ensuring restful holidays. I also want to thank “the Hinderbergers” (Anna, Anja, Lothar, Dennis, Gabi, Luis, Sophia) for being the great south part of our family. Especially I want to thank my grandmother Anna Hinderberger for relieving some of my sorrow after an unpleasant incident.

I would further like to thank all of my friends of Gato Sorriso for getting grounded with samba beats every Thursday evening. Also my old but still best friends deserve my gratitude for giving me new energy on several relaxing sailing trips, winter holidays, or bike tours. Thank you Muffin, Gsell, Schmelzer, Ahmerkamp, Ott, Klein, Schober, Gossens, Fab, and all of you other crazy guys from Goch.

However, my deepest and greatest gratitude goes to my girlfriend, Sarah Schmitz, who suffered with me, motivated me, supported me, and stood with me in any stressful and inconvenient situation. Thank you Sarah for shoudering so much and for loving me through all ups and downs of this journey. Vielen Dank Tle! Ich liebe dich über alles!

Vielen Dank euch allen!
Thank you all so much!
Part III

APPENDIX
A.1 MODEL APPLICATION TO THE RUNNING USE CASE

Figure A.1 shows how the graph can be modeled for the running use case (see Section 5.5.1) with entities $e_1, \ldots, e_{15}$ and their observation channels $o_1, \ldots, o_{31}$ and a disturbance channel $d_1$. Table A.1 shows the allocation of the respective purpose and location properties of each entity node. Additional purposes have been modeled for the fitness app $e_4$, the health app $e_8$, and the fitness service $e_5$. 

Figure A.1: Instantiation of the privacy model for the running use case, representing privacy-affecting entities $e_1, \ldots, e_{15}$ and potential privacy implications of observation channels $o_1, \ldots, o_{31}$ and disturbance channel $d_1$. 

**Table A.1: Entities’ purpose and location properties in the running use case**

<table>
<thead>
<tr>
<th>entity</th>
<th>node</th>
<th>purpose</th>
<th>location</th>
</tr>
</thead>
<tbody>
<tr>
<td>wrist band</td>
<td>e₁</td>
<td>provide vital parameters</td>
<td>&lt;on body&gt;</td>
</tr>
<tr>
<td>smartphone</td>
<td>–</td>
<td>–</td>
<td>48°23'44.2&quot;N 9°59'37.5&quot;E</td>
</tr>
<tr>
<td>GPS sensor</td>
<td>e₂</td>
<td>provide location</td>
<td>&lt;on smartphone&gt;</td>
</tr>
<tr>
<td>acceleration sensor</td>
<td>e₃</td>
<td>provide motion data</td>
<td>&lt;on smartphone&gt;</td>
</tr>
<tr>
<td>fitness app</td>
<td>e₄</td>
<td>provide activity</td>
<td>&lt;on smartphone&gt;</td>
</tr>
<tr>
<td>health app</td>
<td>e₈</td>
<td>provide health stats</td>
<td>Berlin, DE</td>
</tr>
<tr>
<td>health app</td>
<td>e₈'</td>
<td>warn about health state</td>
<td>–</td>
</tr>
<tr>
<td>health app</td>
<td>e₈''</td>
<td>emergency call</td>
<td>–</td>
</tr>
<tr>
<td>social network server</td>
<td>e₆</td>
<td>activity motivation</td>
<td>San Francisco, USA</td>
</tr>
<tr>
<td>friends</td>
<td>e₇</td>
<td>&lt;unknown&gt;</td>
<td>&lt;unknown&gt;</td>
</tr>
<tr>
<td>web server</td>
<td>e₁₁</td>
<td>share video stream on website</td>
<td>Ulm, DE</td>
</tr>
<tr>
<td>anybody</td>
<td>e₁₂</td>
<td>&lt;unknown&gt;</td>
<td>&lt;unknown&gt;</td>
</tr>
<tr>
<td>surveillance camera</td>
<td>e₁₃</td>
<td>capture video stream</td>
<td>48°23'40.7&quot;N 9°59'38.0&quot;E</td>
</tr>
<tr>
<td>surveillance server</td>
<td>e₁₄</td>
<td>store video stream for security</td>
<td>Ulm, DE</td>
</tr>
<tr>
<td>police</td>
<td>e₁₅</td>
<td>access video stream for security</td>
<td>&lt;unknown&gt;</td>
</tr>
</tbody>
</table>
A.2 Model Application to the Working Use Case

Figure A.2 shows how the territorial graph can be modeled for the working use case (see Section 5.5.2) with entities $e_1, \ldots, e_{12}$ and their respective disturbance channels $d_1, \ldots, d_8$ and observation channels $o_1, \ldots, o_{16}$. Table A.1 shows the allocation of the respective purpose and location properties of each entity node. Additional purposes have been modeled for the collaboration system $e_6$ and the

![Figure A.2: Instantiation of the privacy model for the working use case, representing privacy-affecting entities $e_1, \ldots, e_{12}$ and privacy implications of observation channels $o_1, \ldots, o_{16}$ and disturbance channels $d_1, \ldots, d_8$.]

<table>
<thead>
<tr>
<th>entity node</th>
<th>purpose</th>
<th>location</th>
</tr>
</thead>
<tbody>
<tr>
<td>smartphone $e_1$</td>
<td>&lt;unknown&gt;</td>
<td>office 1</td>
</tr>
<tr>
<td>WiFi detector $e_2$</td>
<td>provide phone presence data</td>
<td>office 1</td>
</tr>
<tr>
<td>telephone Alice $e_3$</td>
<td>incoming phone notification</td>
<td>office 1</td>
</tr>
<tr>
<td>telephone Charlie $e_4$</td>
<td>incoming phone notification</td>
<td>office 1</td>
</tr>
<tr>
<td>Charlie $e_5$</td>
<td>&lt;unknown&gt;</td>
<td>office 1</td>
</tr>
<tr>
<td>collaboration system 1 $e_6$</td>
<td>provide video chats</td>
<td>office 1</td>
</tr>
<tr>
<td>collaboration service $e_7$</td>
<td>manage video chats</td>
<td>server room</td>
</tr>
<tr>
<td>$e'_7$</td>
<td>share office presence</td>
<td>–</td>
</tr>
<tr>
<td>$e''_7$</td>
<td>share blurred video stream</td>
<td>–</td>
</tr>
<tr>
<td>collaboration system 2 $e_8$</td>
<td>display video stream</td>
<td>office 2</td>
</tr>
<tr>
<td>Dave $e_9$</td>
<td>&lt;unknown&gt;</td>
<td>office 2</td>
</tr>
<tr>
<td>students $e_{11}$</td>
<td>&lt;unknown&gt;</td>
<td>&lt;unknown&gt;</td>
</tr>
<tr>
<td>colleagues $e_{12}$</td>
<td>&lt;unknown&gt;</td>
<td>&lt;unknown&gt;</td>
</tr>
<tr>
<td>anybody $e_{10}$</td>
<td>&lt;unknown&gt;</td>
<td>&lt;unknown&gt;</td>
</tr>
</tbody>
</table>
The following Listing B.1 provides an example of a complete XML-based channel policy (see Section 7.3) of the smart home system as discussed in Section 5.5.3. The policy specifies details about the entity, about the ten involved channels, about the five purposes, and about five control points. Each purpose statement is modeled by a separate purpose node in our territorial privacy graph, as discussed in Section 6.4.

Listing B.1: Channel policy of the smart home system.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<channelPolicy xmlns="http://www.uulm.de/territorial-privacy">
  <entity type="logical" id="023a68c6-4eba-45d8-8350-c7a9c728de11">
    <name>Smart Home System</name>
    <manufacturer>SmartHome Inc.</manufacturer>
    <hierarchy>
      <childEntity id="d784361-f6c9-45b3-a493-056db936103e" type="hardware.sensor.camera">Living Room Camera</childEntity>
      <childEntity id="05785156-0429-4a16-95ad-a23e9d93f370" type="hardware.output.display">Ambient Display</childEntity>
      <childEntity id="3a9223d5-35b7-44ed-9e7c8c3b0e42" type="hardware.sensor.wifi-detector">WiFi Detector</childEntity>
      <childEntity id="0152f5d5-017f-41a6-a1b7-a07820adad82" type="hardware.actuator.door-opener">Automatic Door</childEntity>
    </hierarchy>
    <location type="relative">
      <building>Alice's apartment</building>
    </location>
  </entity>
  <channelSet>
    <channel direction="in" type="observation">
      <id>7694ddb6-c55b-42ee-9853-e544a8016da7</id>
      <content category="user.dynamic.raw.location.relative">location</content>
      <sourceEntity id="3a9223d5-35b7-44ed-9e7c8c3b0e42">
        <policyReference type="direct">http://192.168.1.131/channel-policy.xml</policyReference>
      </sourceEntity>
      <state>active</state>
      <frequency>continuous</frequency>
    </channel>
    <channel direction="out" type="observation">
      <id>0cc28bc-a19a-4b8c-951c-c27a5dd5f0a7</id>
      <content category="user.dynamic.raw.location.relative">location</content>
      <sinkEntity id="2f6459b-bd21-4501-8a8-7ce7d4550986">
        <policyReference type="base">http://location-service.com/policies/</policyReference>
      </sinkEntity>
      <state>active</state>
      <frequency>continuous</frequency>
    </channel>
    <controlPoints>
      <controlPointInterface type="RESTful-API">
        <base>http://192.168.1.100/control-points/channel/</base>
        <method>POST</method>
        <parameter name="control">
          <value type="grant">grant</value>
        </parameter>
      </controlPointInterface>
    </controlPoints>
  </channelSet>
</channelPolicy>
```
<value type="deny">deny</value>
</parameter>
</controlPointInterface>
</controlPoints>
</channel>

<channel direction="in" type="observation">
  <id>b27e9048-c61a-4b0e-9250-013651d1a494</id>
  <content category="user.dynamic.raw.perception">motion</content>
  <sourceEntity id="4474041d-f5d2-42ec-a966-532c6808e30b">
    <policyReference type="direct">android.resource://com.smart-home.app/raw/policy</policyReference>
  </sourceEntity>
  <state>active</state>
  <frequency>continuous</frequency>
</channel>

<channel direction="in" type="observation">
  <id>e04c1f9a-57f3-4421-8d18-3ec6bbf5260a</id>
  <content category="user.dynamic.raw.perception.visual">video</content>
  <sourceEntity id="d784f361-f6c9-45b3-a493-056db936103e">
    <policyReference type="direct">http://192.168.1.129/channel-policy.xml</policyReference>
  </sourceEntity>
  <state>active</state>
  <frequency>continuous</frequency>
</channel>

<channel direction="in" type="disturbance">
  <id>07259e89-56e4-45b8-92f7-a16955d4b878</id>
  <content category="user.technical">notification</content>
  <sourceEntity id="b1cad448-d20f-441f-bc51-a3d1763731e4">
    <policyReference type="direct">http://192.168.1.68/channel-policy.xml</policyReference>
  </sourceEntity>
  <state>inactive</state>
  <frequency>on-demand</frequency>
</channel>

<channel direction="out" type="disturbance">
  <id>3f7b354e-f094-429f-ac25-dfcd57ab61f0</id>
  <content category="user.technical">notification</content>
  <sinkEntity id="05785156-0429-4a16-95ad-a23e9d9fa37f0">
    <policyReference type="direct">http://192.168.1.141/channel-policy.xml</policyReference>
  </sinkEntity>
  <state>inactive</state>
  <frequency>on-demand</frequency>
</channel>

<channel direction="out" type="disturbance">
  <id>ea5c6166-e1be-4b98-8841-827c7249e0a9</id>
  <content category="user.technical">information</content>
  <sinkEntity id="05785156-0429-4a16-95ad-a23e9d9fa37f0">
    <policyReference type="direct">http://192.168.1.141/channel-policy.xml</policyReference>
  </sinkEntity>
  <state>inactive</state>
  <frequency>on-demand</frequency>
</channel>

<channel direction="in" type="disturbance">
  <id>b0183719-55dd-4e56-897d-67609308346e</id>
  <content category="user.social">visit</content>
  <sinkEntity id="05785156-0429-4a16-95ad-a23e9d9fa37f0">
    <policyReference type="direct">http://192.168.1.141/channel-policy.xml</policyReference>
  </sinkEntity>
  <state>inactive</state>
  <frequency>on-demand</frequency>
</channel>
<sourceEntity id="9b6f49b5-2618-4360-84d2-9dcd7b10efb8"></sourceEntity>

<channel>

<channel direction="out" type="disturbance">
  <id>8cdfcc5e-af96-407f-8035-b53ddc59848c</id>
  <content category="user.social">physical access</content>
  <sinkEntity id="0152f5d5-017f-41a6-a1b7-a07826adad82">
    <policyReference type="direct">http://192.168.1.185/channel-policy.xml</policyReference>
  </sinkEntity>
  <state>inactive</state>
  <frequency>on-demand</frequency>
</channel>
</channelSet>

<purposeStatements>

<purposeStatement>
  <purpose domain="social.sharing">
    <target type="user">SmartHome owner</target>
    <description>The smart home system shares persons' presence with apartment owners.</description>
  </purpose>

  <actions>
    <action type="forward">
      <channelSet>
        <channel direction="in">7694db6-c55b-42ee-9853-e544a8016da7</channel>
        <channel direction="out">09cc28bc-a193-4b8a-93e1-c27a5ddf50a7</channel>
      </channelSet>
    </action>
  </actions>

  <controlPoints>
    <controlPointInterface type="RESTful-API">
      <base>http://192.168.1.100/control-points/purpose/p-10b7fd4fd391</base>
      <method>POST</method>
      <parameter name="control">
        <value type="grant">grant</value>
        <value type="deny">deny</value>
      </parameter>
    </controlPointInterface>
  </controlPoints>
</purposeStatement>

<purposeStatement>
  <purpose domain="convenience.activity-support">
    <target type="user">SmartHome residents</target>
    <description>The smart home recognizes residents' activity.</description>
  </purpose>

  <actions>
    <action type="sense">
      <channelSet>
        <channel direction="in">e04c1f3a-57f3-4421-8d18-3ec6bbf52609</channel>
        <channel direction="in">b27e9048-c61a-4b0e-9250-013651d1a494</channel>
        <channel direction="out">a2cc1f9a-13b1-45c1-a7e0-a2ce10bbae3f</channel>
      </channelSet>
    </action>
  </actions>

  <controlPoints>
    <controlPointInterface type="RESTful-API">
      <base>http://192.168.1.100/control-points/purpose/p-ef446dd0f06b</base>
      <method>POST</method>
      <parameter name="control">
        <value type="grant">grant</value>
        <value type="deny">deny</value>
      </parameter>
    </controlPointInterface>
  </controlPoints>
</purposeStatement>
</purposeStatements>
<purposeStatement>
  <purpose domain="convenience.activity-support">
    <target type="user">SmartHome residents</target>
    <description>The smart home supports residents' activity with information presentation.</description>
  </purpose>
  <actions>
    <action type="use">
      <channelSet>
        <channel direction="in">a2cc1f0a-1381-45c1-a7e0-a2ce10becc3f</channel>
      </channelSet>
    </action>
    <action type="control">
      <channelSet>
        <channel direction="in">a2cc1f0a-1381-45c1-a7e0-a2ce10becc3f</channel>
        <channel direction="out">ea5c61e6-e18e-4bc9-8841-827cf7249d9a</channel>
      </channelSet>
    </action>
  </actions>
  <controlPoints>
    <controlPointInterface type="RESTful-API">
      <base>http://192.168.1.100/control-points/purpose/p-720bd621201a/<base>
      <method>POST</method>
      <parameter name="control">
        <value type="grant">grant</value>
        <value type="deny">deny</value>
      </parameter>
    </controlPointInterface>
  </controlPoints>
</purposeStatement>

<purposeStatement>
  <purpose domain="household.notifications">
    <target type="user">SmartHome residents</target>
    <description>The smart home disseminates notifications of household devices.</description>
  </purpose>
  <actions>
    <action type="trigger">
      <channelSet>
        <channel direction="in">07259e89-56e4-45b8-9277-a16955d4b878</channel>
        <channel direction="out">ea5c61e6-e18e-4bc9-8841-827cf7249d9a</channel>
      </channelSet>
    </action>
  </actions>
  <controlPoints>
    <controlPointInterface type="RESTful-API">
      <base>http://192.168.1.100/control-points/purpose/p-abf69539d20d/<base>
      <method>POST</method>
      <parameter name="control">
        <value type="grant">grant</value>
        <value type="deny">deny</value>
      </parameter>
    </controlPointInterface>
  </controlPoints>
</purposeStatement>

<purposeStatement>
  <purpose domain="security.home-access">
    <target type="user">Authorized persons</target>
    <description>The smart home system automatically opens the front door to authorized persons.</description>
  </purpose>
  <actions>
    <action type="control">
      <channelSet>
        <channel direction="in">b018371f-55dd-4e56-89f7-ed769308346</channel>
        <channel direction="out">8cdffcc5e-af96-407f-8035-b533dd59848c</channel>
      </channelSet>
    </action>
  </actions>
  <controlPoints>
    <controlPointInterface type="RESTful-API">
      <base>http://192.168.1.100/control-points/purpose/p-720bd621201a/<base>
      <method>POST</method>
      <parameter name="control">
        <value type="grant">grant</value>
        <value type="deny">deny</value>
      </parameter>
    </controlPointInterface>
  </controlPoints>
</purposeStatement>
<channelSet>
</channelSet>

</actions>

<controlPoints>
  <controlPointInterface type="RESTful-API">
    <base>http://192.168.1.100/control-points/purpose/p-b6e2796b8f12/</base>
    <method>POST</method>
    <parameter name="control">
      <value type="grant">grant</value>
      <value type="deny">deny</value>
    </parameter>
  </controlPointInterface>
</controlPoints>

<purposeStatement>
</purposeStatement>

</channelPolicy>
The following figures provide screenshots of the German version of the PriVis app as used in our scenario-based evaluation, see Section 9.5. Screenshots in each figure show how the PriVis app can be used to solve the different tasks of our evaluation, see Section 9.5.2.

Figure C.1: PriVis app screenshots, showing how it is used to solve task 2a of the scenario-based evaluation: Which systems in your environment, remote services or persons currently access your position? What is the purpose of access?
Figure C.2: Screenshots of the PriVis app, showing how it can be used to solve task 2b of the scenario-based evaluation: Which inactive remote services or persons could access your position and on what condition?

Figure C.3: Screenshots of the PriVis app, showing how it can be used to solve task 2c of the scenario-based evaluation: Through which sensor(s) is your current position or presence detected?
Figure C.4: Screenshots of the PriVis app, showing how it can be used to solve task 2d of the scenario-based evaluation: You don’t want to store your fitness statistics on the 4YourFitness server anymore. Change the respective settings.

Figure C.5: Screenshots of the PriVis app, showing how it can be used to solve task 3a of the scenario-based evaluation: Who or what can access your activity (e.g., watching TV or cooking) and for what purpose?
Figure C.6: Screenshots of the PriVis app, showing how it can be used to solve task 3b of the scenario-based evaluation: What information/data is required for the recognition of your activity?

Figure C.7: Screenshots of the PriVis app, showing how it can be used to solve task 3c of the scenario-based evaluation: Who or what can access the video stream of the video camera in your apartment and on what condition?
Figure C.8: Screenshots of the PriVis app, showing how it can be used to solve task 3d of the scenario-based evaluation: Which persons can access your locomotion (sitting, standing, walking) and on what condition?

Figure C.9: Screenshots of the PriVis app, showing how it can be used to solve task 4a and 4b of the scenario-based evaluation: Deactivate the cleaning robot. Why did the robot start its cleaning process?
Figure C.10: Screenshots of the PriVis app, showing how it can be used to solve task 4c of the scenario-based evaluation: Are there any further disturbances that could be caused through systems in your environment?

Figure C.11: Screenshots of the PriVis app, showing how it can be used to solve task 4d of the scenario-based evaluation: You want to prevent further disturbances while you are relaxing. What would be your strategy to realize this?
BIBLIOGRAPHY

REFEREED PUBLICATIONS BY THE AUTHOR


REFERENCES


Bibliography


[415] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing facebook privacy settings: user expectations vs. real-


[470] M. Nauman, S. Khan, and X. Zhang. Apex: Extending android permission model and enforcement with user-defined runtime


[516] A. Pfötzmann and M. Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, August 2010. URL http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf. v0.34.


[697] A. Woodruff, V. Pihur, S. Consolvo, L. Schmidt, L. Brandimarte, and A. Acquisti. Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? the


