# BALANCING PRIVACY NEEDS WITH LOCATION SHARING IN MOBILE COMPUTING

KARIM ANTHONY ADAM

A thesis submitted in partial fulfillment of the requirements for
the degree of Doctor of Philosophy in Computer Science

Department of Computing
Faculty of Mathematics, Computing and Technology
The Open University

2009

**Dedication**

*To my sweet little angel, Kana-Maluwe, my dad, and in loving memory of my late mum, sister, and brother.*

**Author's Declaration**

Some of the material in this thesis has been previously published in the following papers:

a. Price, B. A., Adam, K., & Nuseibeh, B. (2005). *Keeping Ubiquitous Computing to Yourself: a practical model for user control of privacy*. International Journal of Human-Computer Studies, 63(1-2):228–253, July 2005.

b. Adam, K., Price, B., Richards, M., & Nuseibeh, B. (2005). *A Privacy Preference Model for Pervasive Computing.* Paper presented at the The First European Conference on Mobile Government, University of Sussex, Brighton, 10-12 July.

All of the work presented in this thesis describes my original contributions, except otherwise stated and referenced.

**Acknowledgements**

I would first of all like to acknowledge my supervisory team, led by Blaine Price, without whose guidance and support this research would not have seen the light of day. The other team members include Prof. Bashar Nuseibeh, Dr. Adam Joinson, and Prof. Marian Petre. I am and will always be very grateful to them for their patience, understanding, and good sense of direction, particularly at times when this work was threatened by life's challenges.

I am also indebted to colleagues of the Mathematics and Computing Faculty of the Open University, in particular members of the PG Forum, (then headed by Prof. Marian Petre and Dr. Trevor Collins) for sharing their research experiences and challenges with me. They include Katerina Tzanidou, Geke van Dijk, Michele Pasin, Mohammed Salifu, Armstrong Nhlabatsi, etc. My Mulberry Lawn team mates John Brier and Zhi Li deserve a special mention for their role in helping bring a balance between research and practice.

I also acknowledge the contributions of various reviewers of parts or all of this research, including Prof. Helen Sharp, Prof. Yvonne Rogers and Dr. Anne Adams for their very useful comments which have helped shape this work. Many thanks to Dr. Michel Wermelinger for being very supportive in his role as my third party monitor and to my dear uncle and mentor, Mr. Moses Mengu, for first believing in me and initiating a research dialogue which eventually led to this piece of work.

I would like to thank various reviewers of my work at workshops and conferences (in particular UK-UbiNet 2005, INTERACT 2005, mGov 2005, CHI 2006, etc), whose comments have helped provide useful pointers in the key milestones of this work.

Finally, my sincere thanks and appreciation go to God for guiding me through yet another major milestone of my life, and a special tribute to my dad, Mr. E.T. Adam, for his confidence in me, and being there for me at all times.

**Abstract**

Mobile phones are increasingly becoming tools for social interaction. As more phones come equipped with location tracking capabilities, capable of collecting and distributing personal information (including location) of their users, user control of location information and privacy for that matter, has become an important research issue.

This research first explores various techniques of user control of location in location-based systems, and proposes the re-conceptualisation of deception (defined here as the deliberate withholding of location information) from information systems security to the field of location privacy. Previous work in this area considers techniques such as anonymisation, encryption, cloaking and blurring, among others. Since mobile devices have become social tools, this thesis takes a different approach by empirically investigating first the likelihood of the use of the proposed technique (deception) in protecting location privacy. We present empirical results (based on an online study) that show that people are willing to deliberately withhold their location information to protect their location privacy. However, our study shows that people feel uneasy in engaging in this type of deception if they believe this will be detected by their intended recipients. The results also suggest that the technique is popular in situations where it is very difficult to detect that there has been a deliberate withholding of location information during a location disclosure.

Our findings are then presented in the form of initial design guidelines for the design of deception to control location privacy. Based on these initial guidelines, we propose and build a deception-based privacy control model. Two different evaluation approaches are employed in investigating the suitability of the model. These include; a field-based study of the techniques employed in the model and a laboratory-based usability study of the Mobile Client application upon which the DPC model is based, using HCI (Human Computer Interaction) professionals.

Finally, we present guidelines for the design of deception in location disclosure, and lessons learned from the two evaluation approaches. We also propose a unified privacy preference framework implemented on the application layer of the mobile platform as a future direction of this thesis.

## Table of Contents

**Dedication** ..... **ii**

**Author's Declaration** ..... **iii**

**Acknowledgements** ..... **iv**

**Abstract** ..... **v**

**Table of Contents** ..... **vi**

**Table of Figures** ..... **x**

**Chapter 1. Introduction** ..... **13**

1.1 Introduction ..... 13

1.2 Research Problem ..... 15

1.3 Research Contribution ..... 15

1.4 Research Scope ..... 16

1.5 Research Strategy ..... 17

1.6 Thesis Structure ..... 17

**Chapter 2. Literature Review** ..... **19**

2.1 Privacy ..... 19

*2.1.1 Historical Perspective* ..... *19*

*2.1.2 Classes of Privacy* ..... *21*

2.2 Origins of legal protection and models of data protection ..... 22

2.3 Models of Privacy Protection ..... 23

2.4 Summary ..... 25

2.5 Privacy in Mobile Computing ..... 25

*2.5.1 Types of Mobile computing Privacy* ..... *26*

2.6 Personally Identifying Information & Mobile computing Services ..... 27

2.7 Classifying Mobile computing Services and Scenarios ..... 28

2.8 Privacy in Mobile computing: Where it hurts most ..... 29

2.9 Privacy Control Technologies ..... 30

*2.9.1 Privacy Matrix* ..... *30*

*2.9.2 Privacy Control Architectures* ..... *31*

2.10 Principles of Privacy Protecting Systems ..... 33

*2.10.1 Requirements from Privacy Principles* ..... *33*

*2.10.2 Deriving privacy principles in mobile computing from the principles of minimum asymmetry and approximate information flows* ..... *34*

2.11 Comparison of Privacy Protecting Models in Mobile computing ..... 36

2.12 Deception in Location Disclosure as a Privacy Control Mechanism ..... 37
*2.12.1 Deception ..... 38*
2.13 Deception and Mobile Computing Privacy ..... 40
*2.13.1 Summary ..... 41*

**Chapter 3. To What Extent Can Deception Control Location Privacy? ..... 42**

3.1 Introduction ..... 42
3.2 Scenarios ..... 42
3.3 Study Objectives ..... 43
3.4 Preliminary Study ..... 44
3.5 Method ..... 45
*3.5.1 Participants ..... 45*
*3.5.2 Materials ..... 46*
*3.5.3 Procedure ..... 46*
3.6 Results, Data Analysis and Findings ..... 47
*3.6.1 Investigating how location is disclosed in general to a requestor ..... 48*
*3.6.2 Withholding Location Information for Good Purposes ..... 50*
*3.6.3 Deception as a Tool to Enhance Social Harmony ..... 53*
*3.6.4 Comparison of Likelihood and Level of Discomfort across All Three Scenarios ..... 57*
3.7 Causes of High Level of Discomfort in the Use of Deception to Protect Location Privacy ..... 58
*3.7.1 Method ..... 58*
*3.7.2 Findings and Discussions ..... 59*
3.8 The Role of Strategic Deception in Location Disclosure ..... 63
3.9 The principle of strategic deception (PSD) in plausible location disclosure ..... 64
3.10 Conclusions ..... 66

**Chapter 4. Deception-Based Location Privacy Control Model ..... 69**

4.1 Introduction ..... 69
4.2 General Overview and Requirements ..... 69
*4.2.1 Working scenario: ..... 69*
*4.2.2 Requirements for the Implementation of Deception ..... 70*
4.3 Deception-based Privacy Control Model ..... 70
*4.3.1 Location Sensing Using GSM Global Cell IDs and GPS Coordinates ..... 71*
4.4 5-layer Disclosure Approach ..... 73
*4.4.1 Usage Scenario ..... 75*
4.5 Implementing the DPC Model ..... 80
*4.5.1 Architecture Component description ..... 81*
*4.5.2 The Mobile Phone Platform ..... 82*

*4.5.3 Location Sensing* ... *82*
*4.5.4 Coding environment* ... *83*
4.6 Functional Testing of the DPC Model ... 83
*4.6.1 Limitations* ... *84*
4.7 Summary ... 85

**Chapter 5. Field-based User Evaluation of the Mobile Client Application ... 86**

5.1 Introduction ... 86
5.2 Objectives of the study ... 86
5.3 Platform ... 86
5.4 Study Design ... 89
5.5 Participants ... 89
5.6 Protocol ... 90
5.7 Data Capture and Analysis ... 93
5.8 Findings ... 93
5.9 Threats to Validity ... 95
5.10 Discussion ... 95
5.11 Conclusion ... 96

**Chapter 6. Usability Evaluation of the Mobile Client Application ... 98**

6.1 Introduction ... 98
6.2 Objectives of the study ... 98
6.3 Methodology ... 98
6.4 The Study ... 99
6.5 Data Capture and Analysis ... 100
6.6 Findings ... 101
*6.6.1 Adding Contacts* ... *103*
*6.6.2 Setting of Disclosure Preferences* ... *104*
*6.6.3 Making a Location Request* ... *105*
*6.6.4 Making a Location Disclosure* ... *105*
*6.6.5 Deleting a contact* ... *106*
*6.6.6 Error Handling* ... *107*
6.7 Platform Problems ... 107
6.8 Threat to Validity ... 108
6.9 Discussions ... 108
6.10 Conclusion ... 109

**Chapter 7. Conclusions ... 110**

7.1 Introduction ... 110

7.2 Goals & Findings ..... 111
7.3 Critical Review of Thesis ..... 111
*7.3.1 Scope ..... 111*
*7.3.2 Methodology ..... 112*
7.4 Contributions ..... 112
7.5 Future Work ..... 114

**References ..... 116**

**Appendix A ..... 123**

**Appendix B ..... 133**

**Appendix C ..... 143**

**Appendix D: Post User Study Responses ..... 155**

**Appendix E: User Consent and Post Study Questionnaires ..... 163**

## Table of Figures

Figure 2.9-1: The Privacy Matrix. Source (Gunter et al., 2004) ..... 31
Figure 3.2-1: Reasons for Scenario-based Design (Carroll, 2000) ..... 43
Figure 3.6-1: Perception of the Use of Disclosure Strategies for Requests Coming from Each Member of the Discloser's Social Network ..... 49
Figure 3.6-2: Mean Likelihood of Disclosing a False Location with a Good Intent ..... 51
Figure 3.6-3: Mean Level of Discomfort after Disclosing a False Location with a Good Intent ..... 52
Figure 3.6-4: Mean Likelihood of Disclosing a False Location to Enhance Social Harmony ..... 54
Figure 3.6-5: Mean Level of Discomfort After Disclosing a False Location to Enhance Social Harmony ..... 54
Figure 3.6-6: Mean Likelihood of Disclosing a False Location for Other Scenarios ..... 56
Figure 3.6-7: Mean Level of Discomfort in Disclosing a False Location for Other Scenarios ..... 57
Figure 3.6-8: Likelihood versus Level of Discomfort across Three Scenarios ..... 58
Figure 3.7-1: Level of Discomfort Vs. Possibility of Deception Discovery ..... 60
Figure 3.7-2: Level of Discomfort Vs. Location Privacy Protection Technique ..... 61
Figure 3.7-3: Ethics Concern Vs. Techniques and Possibility of Discovery ..... 62
Figure 3.9-1: Usage Scenario Describing How a Request and Disclosure are Made Between Two Mobile Client Users. ..... 65
Figure 3.9-2: Process Flow of the PSD Involving Components of the DPC Model's Architecture ..... 66
Figure 4.3-1 A Map Showing GSM Station Mast Positions in Parts of Milton Keynes, UK ..... 72
Figure 4.3-2: Structure of a Cell in Mobile Network Systems ..... 72
Figure 4.4-1: 5-Layer Disclosure Model Based on Cell ID Parameter (Signature) Comparison ..... 73
Figure 4.4-2: Execution Flow of Location Disclosure Process. This describes the flow process for disclosing a location using the Disclosure Matrix (DM) described in Table 4.1. ..... 77
Figure 4.4-3: Disclosure Flow Process by Preferences. This outlines broadly the disclosure of a location, based on the set preferences for a particular request. ..... 78
Figure 4.5-1: Architectural Representation of the DPC Model ..... 81
Figure 4.6-1: Screen Shot From the Test Environment on J2ME Wireless Toolkit ..... 84
Figure 5.3-1: Architecture of Mobile Feedback Operation – (www.mobilefeedback.com) ..... 88
Figure 5.3-2: Mobile Feedback Screen Shot of Log of Active Sessions ..... 88
Figure 5.8-1: Mean Perception of Disclosure by Requestor ..... 95
Figure 6.6-1: Distribution of Total Usability Problems by Severity ..... 102

## List of Tables

Table 2.1: Classes of Privacy ..... 21
Table 2.2: Taxonomy of Data Types and Examples based on(Corby, 2002) ..... 28
Table 2.3: Privacy Principles from the Fair Information Practices ..... 34
Table 2.4: Additional Properties for privacy policy derivation in mobile computing ..... 35
Table 2.5: Comparison of Privacy Protecting Models in Mobile computing ..... 37
Table 3.1: Breakdown of Overall Participation ..... 45
Table 3.2: Breakdown of Responses by Scenarios ..... 48
Table 3.3: Response Rate for General Strategies in Making Location Disclosures ..... 48
Table 3.4: Mean Likelihood and Level of Discomfort for the Disclosure of a False Location with a Good Intent ..... 50
Table 3.5: Mean Likelihood of Disclosing a False Location to Enhance Social Harmony ..... 53
Table 3.6: Mean Likelihood and Level of Discomfort of Disclosing a False Location in Other Scenarios ..... 55
Table 3.7: Summary of Mean Likelihood and Level of Discomfort Across All Three Scenarios ..... 57
Table 3.8: Level of Discomfort for Different Possibilities of Deception Discovery ..... 60
Table 3.9: Mean Level of Discomfort for Various Techniques of Location Privacy Protection ..... 61
Table 3.10: Mean Level of Ethics Concern for High and Low Possibilities of Deception Detection ..... 62
Table 3.11: Disclosure Factors Influencing Strategic Deception ..... 63
Table 4.1: Disclosure Matrix (DM) Based on the 5-layer Disclosure Model ..... 79
Table 4.2: Example of Location Signatures ..... 80
Table 5.1: Disclosure Results from Pilot 1 ..... 91
Table 5.2: Disclosure Results from Pilot 2 ..... 92
Table 5.3:Score Represented by Perception of Disclosed Location to Requestor ..... 93
Table 5.4: Mean Perception of Disclosure by Requestor ..... 94
Table 6.1: Detailed Description of Tasks Used During Usability Study ..... 100
Table 6.2: No. of Usability Problems Identified by each Participant for each Problem Classification ..... 101
Table 6.3: No. of All Usability Problems Identified by Each Participant for Each Task Performed ..... 102
Table 6.4: No. of Usability Problems Discovered by Severity During Contact Addition ..... 103
Table 6.5: No. of Usability Problems According to the Nature of Problem During the Task of Adding Contacts ..... 103
Table 6.6: No. of Usability Problems Discovered by Severity During the Task of Disclosure Preference Setting ..... 104
Table 6.7: No. of Usability Problems According to the Nature of Problem During the Task of Setting Disclosure Preferences ..... 104
Table 6.8: No. of Usability Problems Discovered by Severity During the Task of Making a ..... 105

Table 6.9: No. of Usability Problems According to the Nature of Problem During the Task of Making a Location Request ..... 105
Table 6.10: No. of Usability Problems Discovered by Severity During the Task of Making a Location Disclosure ..... 106
Table 6.11: No. of Usability Problems According to the Nature of Problem During the Task of Making a Location Disclosure ..... 106
Table 6.12: No. of Usability Problems Discovered by Severity During the Task of Deleting a Contact ..... 106
Table 6.13: No. of Usability Problems According to the Nature of Problem During the Task of Deleting a Contact ..... 107
Table 6.14: No. of Usability Problems Discovered by Severity During the Task of Error Handling Evaluation ..... 107
Table 6.15: No. of Usability Problems According to the Nature of Problem During the Task of Error Handling Evaluation ..... 107

# *Chapter 1. Introduction*

## 1.1 Introduction

Throughout history, in a person's daily interactions with his or her environment, location has been crucial to survival. This is true of resources – knowing where the supermarket is, or where wild foodstuffs may be gathered. It is true of dangers – knowing the location of a hazardous bridge or of a prowling predator.

Location is equally important with respect to social interactions, not just in terms of resources and dangers, but also in terms of maintaining social relationships and meeting social responsibilities. Prompt, accurate knowledge of the location of an accident can enable emergency services to save lives. Parents' knowledge of their children's whereabouts may enable them to assess their safety. The communication of location among people within social networks is a common interaction within the social discourse (Smith, 2005).

In the last decade, there is no doubt that technology has played a useful role in improving the way location is communicated between people. A number of technologies (e.g. mobile phone conversations, text or instant messaging, and email) have facilitated the exchange of location information between people of the same social network (Smith, 2005). Studies conducted in Germany and England suggest that teenagers use text messaging to get connected with friends and loved ones, and to arrange meetings (Grinter and Eldridge 2001; Höflich and Rössler 2001; Smith, Consolvo et al. 2005), all of which depend on their physical locations. The underlying principle behind these technologies (i.e. the use of asynchronous communication) has been harnessed into the provision of location-based services (i.e. services that rely on the current location of their users), and in recent times *social location disclosure applications* - SLDA SLDAs usually rely on "the explicit sharing of location information in a social communication" (Smith, 2005). With the use of GSM-based fingerprinting (Laitinen et al., 2001; Otsason et al., 2005) which improves location accuracy to about 43 metres (in urban areas), more location-based services have begun to emerge and are increasingly becoming popular (child location services, fleet management systems, friend finders, etc).

The upsurge in the provision of location-based services by mobile phone operators in particular comes with benefits which have never been as promising as they are now. In 2005 revenue from

location-based services in Europe was 274 million Euros. This figure is expected to reach 622 million Euros by 2010 (Berg Insight, 2006).

Much as these services provide social as well as financial benefits, one major setback threatens their use – the ability to control one's location privacy. The lack of user control of location in location-based services such as the friend finder makes it difficult for users to manage their location disclosures effectively, other than a **disclose/do not disclose** setting. Since location can be sensitive personal information, disclosure can be a source of privacy risk. For instance, knowing that a teenage girl is located in a pregnancy crisis centre could potentially tell a lot about the person.

In a recent survey of location-based service providers, more innovative location-based services to meet user needs was cited as one of three key factors that will further help boost the market for location-based services (Berg Insight, 2006). Though this was a marketing survey, and hence, less reliable than an academic survey, it is clear that addressing inherent problems in location-based services through innovative user control models is a market enabler and should be given considerable attention in the research environment.

In this thesis I have therefore chosen to focus on privacy as a key issue to investigate. Previous studies indicate that users of location-based services generally control their location disclosure by *anonymising* (hiding the identity of the user); *blurring* (decreasing the accuracy of the location and possibly time; *cloaking* (making the user's location invisible); *encrypting or hashing* (disguising or obscuring the identity or location of the user); or *lying or benign deception* (giving intentionally false information about location or time). A substantial amount of work has already been carried out in anonymising (Beresford & Stajano, 2003; Gruteser & Grunwald, 2003); blurring (Duckham & Kulik, 2005; Gruteser & Grunwald, 2003); cloaking (Gruteser & Grunwald, 2003; Hong & Landay, 2004); and encryption (Beresford & Stajano, 2003; Jorns & Bessler, 2004). Most of these mechanisms are more suited for person-to-organisation interactions rather than peer-to-peer asynchronous setups where users request for their friends' locations through their mobile devices instead of making a request from a web-based interface. I focus my research on deception as a location privacy protection mechanism because I find deception as an interesting social phenomenon. Besides, research in deception during location disclosure is just beginning to attract some attention among researchers in pervasive computing (Benford et al., 2004; Iachello et al., 2005), though no work has yet been done on the use of deception in particular, as a design technique to protect location privacy.

## 1.2 Research Problem

As stated above, though a substantial amount of work has been carried out in the use of deception in other disciplines, very little research has been done in location–based systems. There is already ample empirical evidence that deception (or put loosely, the disclosure of an untrue location during social interactions) is popular between people who communicate asynchronously. However, one of the pitfalls of designing location-based systems is *the inhibition of established practice* (Lederer et al., 2004). Lederer and his colleagues have therefore described in their work that such "designs should not inhibit users from transferring established social practice to emerging technologies." This research is in part based on the spirit of the above statement.

In this thesis I have articulated location privacy as a problem in the use of location-based applications. To this end, I have proposed a user-control model based on the use of deception to protect location privacy by first investigating the use of deception as an established social practice in location disclosure. Having also been established as being an effective tool in information systems security through the use of honey pots (Cohen et al, 2005), deception is yet to become a design consideration in social mobile computing including location disclosure.

The main question that this research answers is:

*How can privacy needs be balanced with location sharing in mobile computing?*
This question investigates the extent to which privacy requirements and/or expectations of users of location-based services are met while sharing their location information with other users.
Therefore in order to explore answers to the above question, the following questions were first investigated.

1. What techniques can be used to protect location privacy?
2. To what extent can deception be used to protect location privacy?
3. What factors influence the use of deception to protect location privacy?
4. How can deception be implemented in social mobile computing?

## 1.3 Research Contribution

The key contributions of this research are:

i. The recontextualisation of the notion of deception from classical military warfare and the information systems security environments to location sharing in mobile computing, supported by empirical studies and the literature. This contribution also demonstrates that deception is a technique that can be used to protect location

privacy (see research sub-question 1 above) and also provides evidence of how the privacy requirements or needs of users of location-based services are met during location sharing, using deception as a means of doing this.

ii. The design and implementation of a deception-based privacy control (DPC) model to protect location privacy. The DPC model provides further evidence of how deception can be employed practically on a mobile platform. The model also provides a proof of concept and the practical extent to which deception can be used to protect location privacy in mobile computing (see research sub-question 2 above). An instantiation of the DPC model in the form of an application called the Mobile Client (MC) further demonstrates how deception can be implemented in social mobile computing (reference to research sub-question 4 above).

iii. Empirical validation of the DPC model in the form of a user study and an expert usability evaluation. The empirical data also demonstrates that likelihood and discomfort affect the use of deception to protect location privacy (reference to research sub-question 3 above).

## 1.4 Research Scope

The complex nature of privacy makes it difficult to protect. This becomes even more difficult in the complex technological environment presented by mobile computing. Hence, this thesis does not seek to address all aspects of privacy protection within the mobile computing environment. Instead, it contributes to earlier efforts by other researchers, and has demonstrated that established social practices can be supported by technology.

The deception-based model described in this thesis (see Chapter 4) is limited to asynchronous communications among people of the same social network. It specifically protects the location privacy of individuals engaged in the request/disclosure dialogue. Hence, any generalisation of the use of this model can only prove effective in such environments.

Furthermore, the prototype described in Chapter 4 is developed to work in MIDP 2.0 (Mobile Information Device Profile 2.0) compatible environments. The prototype is evaluated in a field-based user study (in Chapter 5) using people who are actively involved in text or instant messaging. The use of a small focused group as evaluators does not completely extrapolate the model to the

wider population, but instead, proves within the group studied, the effectiveness of the use of deception to protect location privacy.

## 1.5 Research Strategy

The research process chosen in this thesis mainly follows five key Action Research steps (Susman and Evered 1978; Jarvinen 2000; Fléchais 2005). Action Research *is a structured research approach that "identifies a question to investigate, develops an action plan, implements the plan, collects data, and reflects the findings of the investigation*" (Johnson 1995; Fléchais 2005). The following is a brief description of each of the steps involved in Action Research as employed in this research.

a. *identifying* a research question (diagnosing) – this process was largely exploratory in nature, where the research problem was articulated from gaps in available literature, presentations and discussions at conferences and workshops, etc. This step sought to answer research questions 1 and 2 (see Section 1.2).
b. *developing* an action plan (action planning)- this involved the development of a workable timeline for each task that will eventually lead to answering the research questions identified in (a) above.
c. *implementing* the plan (action taking) – This stage involved two online exploratory studies to establish the need for deception as a privacy control strategy, and the development of a deception-based location privacy control model as a prototype.
d. *gathering* and analysing the data (evaluating) – Data in (c) above was collected and analysed to provide empirical evidence of the effectiveness of the proposed model. Steps (b), (c), and (d) all contribute to providing an insight into the solutions of research questions 3 and 4 (see Section 1.2).
*e.* *Reflecting* on the findings of the investigation (specifying learning) – The results of step (d) were used to further draw a conclusion on the significance of the contribution this thesis makes to location privacy protection.

## 1.6 Thesis Structure

This thesis is structured along the same lines as the action steps outlined in Section 1.5.

Chapter 2 surveys related literature and discusses the evolution of location privacy from the technological viewpoint to the introduction of established social practices in the design of privacy protection systems.

Chapter 3 describes a large scale scenario-based online study to determine the effect the use of deception has on *discomfort* and *likelihood*.

Chapter 4 describes the overall deception-based privacy control (DPC) model upon which this thesis is based. It discusses two key strategies of deception (ambiguity and mis-direction strategies), strategic deception, and how the combination of these can provide a new way of ensuring plausible deniability whilst preserving existing social relationships.

The rest of the chapters are based on the evaluation of the DPC model representing:

i. A user view of the model – Chapter 5 outlines a field-based user study of investigating the usefulness and effectiveness of the DPC model.
ii. An expert view of the model – Chapter 6 describes a usability study of the use of the Mobile Client application: a prototype developed to demonstrate the proposed model in Chapter 4.

Finally, Chapter 7 concludes with key contributions of this research, a critical review of the thesis, and future work.

# *Chapter 2. Literature Review*

*"To tell the truth is a duty, but it is a duty only toward one who has a right to the truth."*

*- Immanuel Kant*

## Introduction

This chapter discusses privacy in general (and in particular, location privacy) and its implications on users of mobile devices. Various attempts by researchers to control or protect location privacy are explored here. It is the result of an exploratory study of relevant literature for this research. It begins with an in-depth discussion of privacy from the historical perspective, the origins of legal protection and a number of technologies used in protecting privacy in general (Sections 2.1 – 2.4). This chapter also discusses privacy with specific reference to mobile computing and ends with key research challenges in this area. This is followed by a look at some emerging technologies for privacy control in mobile computing and the introduction of the concept of privacy protecting noise to protect user privacy. Section 2.12 explores the use of deception as a privacy control mechanism, drawing from research in social psychology and the moral justification of deception in the major religions of the world. A short summary concludes the chapter raising potential issues on the nature of research in this direction.

## 2.1 Privacy

This section describes an overview of privacy in the general context beginning with a brief historical perspective, a definition of privacy for the purpose of this study, and ending with the use of technology to protect privacy.

### *2.1.1 Historical Perspective*

The notion of privacy is not new. All through history, privacy has been mentioned either in explicit terms or recognised as part of a set of norms of a particular group of people. The Quran mentions privacy as a right of everyone (Hassan, 1996); Jewish law recognised privacy many years ago as *being free from being watched* (EPIC, 2002; Spitz, 1987); Mikhail Bakhtin (in *Creation of a Prosaics*) describes a person in terms of ancient Greek romance as an "isolated and private individual"(McDougall, 2004; Morson & Emerson, 1991); and the Bible also makes several references to privacy in (Hixson, 1987; McDougall, 2004; Moore, 1984).

Privacy comes from the Latin word, *privatus,* meaning "withdrawn from public life, deprived of office, peculiar to oneself", as opposed to *publicus* (which comes from *pubes,* meaning "the adult population" ) (Harper, 2001). The English word *private* did not exist until 1450 when it was first recorded (McDougall, 2004).

Privacy is often perceived by many researchers as a hydra-headed multidisciplinary concept with observations and conceptions drawn from law, sociology, psychology, anthropology, and in recent times, information and communications technology. The notion of privacy is very much context-dependent and varies across cultures and from person to person (Gordon, 2003). It therefore has no one-size fits-all definition (Lederer, 2003; Westin, 1967). Over the years, political and technological changes have helped shape the meaning of privacy (McDougall, 2004).

Whereas Gavison (1984) described privacy in terms of control (*Solitude*: control over one's interpersonal interactions with other people; *Confidentiality*: control over other people's access to information about oneself; *Autonomy*: control over what one does, i.e., freedom of will), Boyle (2003) in his attempt to deconstruct the meaning of privacy, extended Gavison's notion of control to include attention, fidelity, and identity, respectively.

Whilst privacy is viewed by some as a "normalising, dynamic, social, dialectic process regulating self-environment interactions" (Altman, 1975), others have described it as a continuum between participation and non-participation in a social practice (Pedersen, 2004). Goffman writes about the selective disclosure and withholding of personal information in which people present different personal fronts for each audience they come into contact with (Goffman, 1959).

Perhaps one of the most revealing definitions of privacy was a modified version of Eli Noam's definition (Noam, 1997), by Jiang et al (Jiang et al., 2002) in which privacy is defined as

*"a highly fluid concept about controlling the dissemination and use of one's personal information, one that often involves tradeoffs with efficiency, convenience, safety, accountability, business, marketing and usability."*

The multidisciplinary nature of privacy makes it difficult, if not impossible to provide a definition that is accepted across domains. Nevertheless, it is useful to define the aspect of privacy that this thesis intends to investigate. For the purpose of this work, I define privacy in the words of Westin as *"the claim of individuals, groups or organisations to determine for themselves when, how, and to what extent information about them is communicated to others"* (Westin, 1967).

The above working definition has been articulated in (Bellotti & Sellen, 1993) in which privacy, described as a user interface design issue, is based on key design principles of *feedback* and *control.* However, Adams (2001), in her work on privacy in multimedia environments argues "*that the control and feedback approach to privacy negates the importance of the trade-off that users make in certain situations."* She suggests the significance of including *contexts* in any definition of privacy.

### *2.1.2 Classes of Privacy*

Many attempts have been made to classify privacy in many different ways. Pedersen for instance, classifies privacy into solitude, isolation, anonymity, reserve, intimacy with friends, and intimacy with family (Pedersen, 1999 ). However, this classification does not reveal the broad issues underpinning private data classification in mobile computing, since the individual's physical space or the communication of private information is not taken into account. The Electronic Privacy Information Center (EPIC) classifies privacy into four distinct types (EPIC, 2003). Apart from being comprehensive in its range of issues covered, their classification includes the type of privacy that is of relevance to this document (i.e. information privacy). Table 2.1 below describes the four classes of privacy according to EPIC.

Table 2.1: Classes of Privacy

| Class of Privacy | Description |
|---|---|
| **Information privacy** ***(also termed data protection)*** | describes rules that govern the way personal data is collected and handled e.g. data such as *"*credit information, and medical and government records" |
| **Bodily privacy** | involves "the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches" |
| **Privacy of communications** | describes "the security and privacy of mail, telephones, e-mail and other forms of communication*"* |
| **Territorial privacy** | concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space e.g. searches, video surveillance and ID checks |

## 2.2 Origins of legal protection and models of data protection

During the 1930s and 40s, IBM-Hollerith punch card technology was used by many European governments to process national census data. Following the outbreak of the Second World War, this information was used by the occupying Nazis to identify Jews for transport to extermination camps (Black, 2001). As a result of this and other human rights abuses, post-war Europe codified strict privacy protection through international treaty and national legislation. Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) (EU, 1950) explicitly states that every citizen possesses an intrinsic right to their privacy in both private and family life (subject to some restrictions). The advent of information technology in the 1960s and 1970s saw an increase in the interest in the right to privacy. The first modern data protection law was enacted by the small German state of Hesse in 1970. Then countries like Sweden followed in 1973. These data protection laws gave rise to the evolution of two major international data protection instruments (EPIC, 2003), namely, the Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (EU, 1981) and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (OECD, 1980).

Most Western countries have followed suit, utilising OECD Guidelines (OECD, 1980), often cited as Fair Information Practices (FIP). Western European democracies were early adopters of the OECD guidelines on privacy, influencing the development of European Community (EC) law on data protection and privacy.

Since laws affecting privacy and data protection vary from country to country, four legal jurisdictions (or regulatory regimes) have been identified according to research literature. They include:

1. **States with strong privacy protection including location-awareness:** These states employ a combination of comprehensive national data protection laws (which also include location privacy protection) and sectoral laws (see Section 2.3 below). Examples include the EU and Japan;
2. **States with strong privacy protection:** Generally, such states have comprehensive national data protection laws which may be combined with sectoral laws for effective privacy protection (e.g. Australia and Canada);
3. **States with some privacy protection:** Largely a patchwork of laws which are usually sectoral and some self-regulation by industry (e.g. the USA);
4. **States with little to no privacy protection in law:** These states mostly have some kind of privacy protection as enshrined in the United Nations declaration on human rights, but lack regulation on data protection (e.g. Ghana).

European privacy laws attempt to implement 'transitive closure' whereby data may only be exported from one country to a second country possessing an equivalent data protection regime; or where the exporter has entered into a special data protection contract with an importer willing to provide equivalent protection to that found in the directives (Price et al., 2005; SafeHabour, 2004).

Japan has one of the greatest take-up of consumer-level mobile computing (in the form of location-aware mobile telephone services). It was one of the first countries to define privacy regulations for mobile computing. Early market certainty resulted in increased business confidence and thus a wide proliferation of services. Similarly, thanks to well-established regulation, consumer confidence in new services was higher than in a completely unregulated arena (Milberg et al., 1995)

Canada and Australia have also instituted strong privacy laws, although without explicit mention of location-aware computing. Like the EU and Japan, each country has instituted Information/Privacy Commissioners with the power to take both punitive and retributive action against privacy violations.

Worldwide, regulations requiring mobile telephone networks to provide location information to emergency services (e.g. E-911 in the US, E-112 in Europe) are likely to affect how privacy-enhancing technologies can be applied.

## 2.3 Models of Privacy Protection

Privacy protection can be achieved through the use of laws, codes of practice, and technologies. Detlev Zwick and Nikhilesh Dholakia (1999) have described two models of privacy in the digital age. These are *regulatory* and *self-regulatory*. The regulatory model is described as a standard set of regulations for privacy protection, mainly for EU member countries. A self-regulatory model is based on businesses in the US, the EU and the Federal Communications Commission (FCC) of the US. According to the Electronic Privacy Information Center (EPIC), however, privacy protection models can be classified as being part of a comprehensive law, sectoral law or a self-regulation (EPIC, 2003). These are each described briefly below.

1. **Comprehensive Laws:** These are laws that are often enacted for both public and private sectors to protect personal information from collection, use and dissemination. The European Union adopts this model to ensure compliance with its data protection laws. These laws include:

a. ***Directive 95/46/EC (1995)*** which ensures that users have access to all data held about them; that data is only collected with the individual's explicit consent, and that it is destroyed when it is no longer needed for the original purpose. This directive has possible consequences for location-aware computing. For example, a user enters an area offering a service to which they must subscribe; must the user give explicit permission for the release of personally identifiable data for each new instance of the service? It is possible that this law may protect users, but it is insufficiently flexible for them to effectively utilise the inherent advantages of mobile technology.

b. ***Directive 2002/58/EC (2002)*** which anticipates some measure of technological change. It extends Directive 95/46/EC into the telecommunications sector and makes explicit mention of location-aware technologies. The drafters of this directive were considering second and third-generation mobile telephones, but it is so drafted that it effectively prohibits the use of location information without the user's explicit informed consent. Directive 2002/58/EC requires that equipment and service providers offer a simple free-of-charge method for users to temporarily hide their location information. The directive also controls the use of cookies in web browsers which can be used to recover the browsing activities of an individual user. Another category of this model exists in countries like Canada and Australia often termed a "co-regulatory model" whereby privacy protection rules are developed and enforced by the industry and overseen by privacy agencies of those countries.

2. **Sectoral Laws:** Unlike other Western countries, countries like the US do not possess a comprehensive national data protection law; the closest equivalent to a national privacy commissioner is the Federal Trade Commission (FTC). Instead, these countries have sectoral laws which govern, for instance, children's information online, video rental, or financial information. The disadvantage in this model is the need to enact laws when a new technology emerges. Sectoral laws are used in many countries to further strengthen privacy protection by complementing comprehensive laws. Privacy protection in the United States in particular, consists of a patchwork of legislation at both state and national levels covering distinct, narrow domains; including websites aimed at children (Children's Online Privacy Protection Act, 1998), financial sites (Gramm-Leach-Bliley Act, 1999), health insurance sites (Health Insurance Portability and Accountability Act, 1996), and certain baffling collections of data such as archives of videotape rentals (Video Privacy Protection Act, 1988) (Price et al, 2005).

Given the weak standards set for simple online privacy protection, there is no immediate prospect of legislation in the US either affording any privacy protection or impediment to location-aware computing.

3. **Self-Regulation:** Industrial bodies usually have their codes of practice and various policies for data protection. However, such codes are often found to provide weak protections and enforcement is sometimes a major barrier to effective protection.

## 2.4 Summary

In this section, we have provided a general discussion of privacy from a historical perspective to current models of privacy protection. In the mobile computing environment, the timeliness and accuracy of location information make privacy an issue of greater concern than static online environments. The next sections take a look at location privacy in mobile computing.

## 2.5 Privacy in Mobile Computing

This section explores privacy with specific reference to mobile computing. It classifies mobile computing privacy in Section 2.5.1, gives an overview of technologies that have the potential of being privacy-invasive, and a classification of what constitutes personally-identifiable information and mobile computing services. The section concludes with a brief discussion of a research agenda of privacy in mobile computing.

Mobile computing is in effect defined as, "*using a computing device while in transit*." (ZDNET, 2008). It is the concept of making computers available throughout the physical environment while keeping them invisible to the user (OnlineDictionary, 2005). Mobile computing is the new and 3rd wave of computing. The 1st wave consisted of many users to a single computer (mainframe era); the 2nd wave of computing consisted of one computer to a user; and finally, the 3rd wave is having many computers to one user. Mobile computing is a subset of *ubiquitous computing* (defined as computing anytime, anywhere), which was first articulated by Mark Weiser in 1988 at the Computer Science Lab at Xerox PARC (Weiser et al., 1999).

The invisible nature of mobile computing makes it difficult to see where information is flowing and therefore how it is being used (Weiser et al, 1999). A simple action, such as entering a shop, may reveal a stream of private data without the user's knowledge of data collection, its destination, and without the option for user control. Others say that the use of location-based services in mobile computing presents a double-edged sword, in which there exists a trade-off between enhanced quality of life and privacy (Junglas & Spitzmueller, 2005). While some mobile computing research

projects explicitly address privacy (Esler et al, 1999; Abowd & Mynatt, 2000), so far solutions have been ad hoc and specific to the systems at hand (Langheinrich, 2001).

### *2.5.1 Types of Mobile computing Privacy*

Mobile computing privacy can be broadly classified as *location privacy* and *context privacy*. Location privacy arises from the use of location-based services. Location-based services (LBS), according to the EU technical report on security and privacy for the citizen in post-September 11 digital age (Clements et al., 2003), are classified as:

1. **Emergency services** – With these services the location of a caller can be immediately transmitted to the emergency service provider. Examples include services provided by public services, including police, fire brigades, medical rescue applications, mountain rescue, or telephone help-lines.
2. **In-car services** – This applies to cases where drivers and passengers get traffic, parking and navigation information, weather conditions, yellow pages, medical or breakdown assistance. The car's position could also be monitored for assistance such as theft recovery.
3. **Location information services** –Information is requested by users for events and services provided in a particular location of interest. Examples of such services may be "where is the nearest restaurant, ATM, etc?"
4. **Tracking and tracing** – For improved efficiency and competitive advantage, companies may track and trace their truck fleet and courier management. This could also be used to track children and family members with some degree of accuracy.

Barkhuus & Dey (2003) on one hand, have classified LBS as *location-tracking* services (in which the user's location is tracked by other parties) and *position-aware* services which are based on the device itself having knowledge of its own location. This latter classification gives a broader meaning to the use of LBS in mobile computing. As such, any mention of LBS in this document will be made with reference to Barkhuus & Dey's (2003) classification.

Context privacy arises out of context of use of personal information. Since "the identity of a person gives a lot of second level type of contextual information" (Gross & Specht, 2001), highly sophisticated context-aware applications that hold information about users' interests, preferences, knowledge and detailed activity logs can bring about serious privacy concerns. Time plays a key role in context-aware applications and information about the time of certain activities can compromise privacy of personal information. Examples include working hours versus weekends, as well as mapping the calendar of a person to get information about free versus busy hours (Gross & Specht, 2001). Finally, the environment or activity of an interaction also describes context, and

knowledge about such information in some cases may constitute a privacy concern (Spinney, 2004).

Lessig describes privacy to be shaped by a number of forces, of which technology is one (Lessig, 1998). The next section describes some of these technologies that may be considered to be privacy-intrusive.

## 2.6 Personally Identifying Information & Mobile computing Services

Personally identifiable information (PII) is defined as *"information that can be used to locate or identify an individual, such as names, aliases, Social Security numbers, biometric records, and other personal information that is linked or linkable to an individual"*.

PII is often subjective. There is usually some amount of information whose access requires control by their owners (subjects); PII can range from the identity of an individual to their shopping habits. PII extends only to those items that can be directly or indirectly linked to a single person (or in EU-speak a "natural person") and does not include aggregated anonymous data. I use the term *attacker* to denote a person or organization who seeks to obtain PII without the consent of the owner. In order to consider what PII must be protected, one must first analyze the categories of data linked to an individual. Corby (2002) classifies private data into *static, dynamic, and derived* data. I present an extended version in Table 2.2 below.

As the table shows, mobile computing *sightings* occupy the *dynamic* slot; adding one new data item composed of two parts: *timestamp* and *location*. This can be further divided by how data are used: either *real-time* (where the implied timestamp is "now") or as a *historical* record. It must be noted that dynamic/historical data are not a new privacy risk; it has been available through such mundane IT applications as credit card and telephone records. Mobile computing does, however, have the potential to provide far finer detail about one's location with much greater temporal precision.

It should also be noted that mobile computing implicitly occupies parts of the *derived* data category since analysis of location data over time can yield crucial PII to an attacker. This classification motivates our examination of mobile computing services in the next section.

Table 2.2: Taxonomy of Data Types and Examples based on(Corby, 2002)

| **Type of Data** | | | **Sub-Type & Example** |
|---|---|---|---|
| **Static** | **Identity** | **Offline** | 1. *Bio-identity*: fingerprints, race, colour, gender, height, weight, physical characteristics, retinal pattern, DNA<br>2. *Financial identity*: bank accounts, credit card numbers<br>3. *Legal identity*: government ID numbers (SSN, Passport #, Driver's Licence)<br>4. *Social identity*: membership in church, auto clubs, ethnicity<br>5. *Relationships*: child of, parent of, spouse of<br>6. *Real Property Associations*: home address, business address |
| | | **Online** | *Digital ID*: pseudonym, E-mail address, Username, IP address, Password |
| | **Assets** | **Tangible** | *Property*: buildings, automobiles, boats, mobile phones<br>*Personal Worth*: credit balances, stock portfolios, debt balances |
| | | **Intangible** | *Non-real property*: insurance policies, employee agreements |
| **Dynamic** | **Historical** | | *Low Resolution: Transactions*: financial, travel, mobile phone records<br>*High Resolution: Mobile computing Sightings log (Time, Place)* |
| | **Real-Time** | | *Mobile computing Sightings ([Now], Place)* |
| **Derived** | **Analyzed** | | **Data derived by analyzing trends over time**<br>***Financial behaviour***<br>1. *Trends and changes*: month-to-month variance against baseline<br>2. *Perceived response to new offerings*: matched with experience<br>***Social behaviour***<br>*Behaviour statistics*: drug use, violations of law, family traits<br>***Tastes***<br>*Buying patterns*: purchase of item in a certain class suggests desire to buy other items in same class |
| | **Composed** | | **Linking Data about person to other data**<br>1. *DNA analysis:* DNA linked to human genome database infers tendency to disease, psychological behaviour<br>2. *Multi-Data linking*: e.g. knowing a device with a given MAC address was seen at a given place/time and knowing that the number is registered to a person infers person was at place/time |

## 2.7 Classifying Mobile computing Services and Scenarios

Until recently, the lack of actual mobile computing services available to the general public has meant that much of the work in mobile computing privacy has used hypothetical scenarios analyzed as case studies. In this work, I re-use some of the popular scenarios which represent the range of activities available to a mobile computing user of a device with an explicit user interface. I classify them according to the type of data and how the service affects the user. I only consider scenarios where there is a privacy risk from data processing taking place beyond the user's control. Therefore I do not investigate mobile computing services achieved entirely by computation on the user's device.

Gunter et al. (2004) present four scenarios similar to those found in other work: *FriendsInTown.com, Market Models, What's Here?,* and *Travel Archive*.

1. *FriendsInTown.com* is an alerting service allowing two people to register an interest in being notified when they are close to one another. As soon as the criterion is satisfied both users are informed. Similar scenarios proposed in other work also involve being interrupted by a mobile computing device once a location-based criterion is satisfied. These might include advertising notifications where a user is alerted as they approach a product on sale, or a form of semi-automated check-in as one enters an airport.

2. *Market Models* provides historical information about characteristics of a group of users who satisfy a certain time/space criterion; such as the average income of everyone at Penn Station at noon on a given day.

3. *What's Here?* is typical of services which provide more detail information to a user in response to a request about their present location. Examples include a list of forthcoming events in a building, tourist points of interest (e.g. (Hong & Landay, 2004) among others), or the route to the nearest sushi restaurant (Duckham & Kulik, 2005).

4. *Travel Archive* keeps a record of the datestamps and locations of people in order to answer queries like "where was I this time last year?" or "How many sales people did we have in the Birmingham area on Tuesday?"

According to the data breakdown in Table 2.2 in the *Dynamic* section it is clear that *FriendsInTown.com* and *WhatsHere?* are both examples of Real-Time data, while *MarketModels* and *Travel Archive* rely on historical data. Mobile computing does not bring many new issues with respect to Dynamic Historical data other than the possible increased resolution of sightings. Access to and analysis of the data does not require a mobile computing device. For the Real-Time scenarios, there are clearly two types of service: *Interrupt-Based*, where the user is alerted once certain criteria are satisfied, and *Query-Based,* where the user asks for information based on their current location.

## 2.8 Privacy in Mobile computing: Where it hurts most

The above discourse on privacy control in mobile computing presents us with three interesting and significant areas that form a broad spectrum of issues in a research agenda of privacy in mobile computing. These are:

1. **Noise:** The inclusion of noise (anonymising, cloaking, blurring, encryption, and lying) as a privacy preference.
2. **Regulatory Regimes:** Recognition of the data protection jurisdiction (DPJ) as an important factor that influences user privacy preferences in a typical mobile computing interaction where participants travel across borders. Encoding relevant laws for various jurisdictions can help reduce false positives in privacy preference settings without users having to understand these laws. False positives occur when an unnecessary alarm is triggered for an event which should be considered privacy-friendly or privacy neutral (see (Adam et al., 2005)).
3. **Economic Model**: The need to cater for a mismatch between privacy preferences of users and privacy policies of LBS. The evolution of this model is deeply-rooted in the economics of privacy (see (Acquisti, 2004), which has undergone a conceptual transformation shaped by technology.

A more detailed discussion of the above can be found in (Adam et al., 2005).

## 2.9 Privacy Control Technologies

This section discusses privacy control technologies in mobile computing. Section 2.9.1 describes the principles of access, use, and collection in a privacy matrix. The privacy matrix is a useful starting point for privacy-sensitive designs. Section 2.9.2 critically examines the use of some privacy control architectures in mobile computing. This is then followed by the principles of privacy protecting models in mobile computing (Section 2.10), and ends with a comparison of privacy protecting models in mobile computing (Section 2.11).

### *2.9.1 Privacy Matrix*

Gunter et al (2004) present a privacy matrix for location-based services consisting of three axes as illustrated in Figure 2.9-1 below. The privacy matrix represents a solution space for the design of privacy-sensitive architectures. The authors argue that every privacy-related issue in mobile computing occupies a spot in a 3D space (called the privacy matrix) below. This is true to a large extent if we go by my earlier definition of privacy in S 2.1.1. The next section discusses some privacy control architectures in mobile computing.

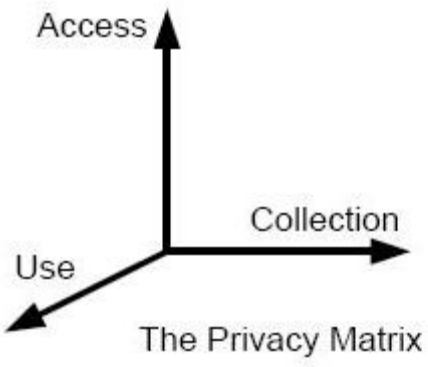


Figure 2.9-1: The Privacy Matrix. Source (Gunter et al., 2004)

### *2.9.2 Privacy Control Architectures*

In the last decade there has been an increased interest in privacy-related research in mobile computing. A number of privacy-preserving, privacy-enhancing, and privacy-protecting technologies have been proposed, some of which have been implemented in mobile devices (e.g. (AT&T, 2003)). Ackerman (2004) describes these technologies in four broad categories, namely: *encryption and security mechanisms, anonymising mechanisms* (Beresford & Stajano, 2003; Gruteser & Grunwald, 2003)*, infrastructures* (Hong & Landay, 2004; Langheinrich, 2002; Yamada & Kamioka, 2005), *and labelling protocols* (Cranor, 2002).

Jiang et al. (2002) categorise privacy-protecting technologies into three types: *prevention, avoidance,* and *detection*. The authors also separate the lifecycle of personal data into three phases: *collection, access,* and *second use*. The three types of privacy protection mechanism together with the three lifecycle phases combine to form a "design space" of privacy solutions divided into nine two-dimensional zones. Jiang and his colleagues further stress that previous mobile computing privacy research has explored only a small portion of the entire design space; primarily preventive mechanisms for the collection and initial access of data. They point out that there is the need to explore other areas such as controlling the second-use of personal data, and measures for detecting unauthorized access of personal data.

Under Ackerman's classification, infrastructure-based privacy-protecting technologies usually make use of a combination of the technologies listed above. Next, I take a look at a number of such infrastructures used in mobile computing.

The Confab System (Hong & Landay, 2004) provides a framework for end-users and application developers to manage privacy within mobile computing. Confab is probably the most recent and most advanced privacy-sensitive architecture (Ackerman, 2004). Confab's architecture is based on a decentralised approach for building control and feedback mechanisms as well as a form of

'plausible deniability' allowing for exceptions to the emergency services. Although Confab is robust and supports a wide range of mobile computing applications across pessimistic, optimistic and mixed-initiative environments; it only supports relatively simple *privacy preferences* (Ackerman, 2004). A privacy preference can be defined as the choice of what personal information about an individual should be revealed, how long such information should be retained and for whom it should be revealed. Whilst a pessimistic environment is a situation where an application prevents abuses, an optimistic application detects abuses of personal information. In the case of mixed-initiative environments, information-sharing decisions are made by end-users. Pessimistic mobile computing applications rely on users configuring their privacy preferences beforehand. The setback in such applications is the unavailability of a common language that supports the expression of multiple privacy preferences.

Langheinrich (2002) discusses a privacy awareness system, or *pawS*, which supports privacy in ubiquitous computing. The user's device is equipped with a personal privacy assistant which handles the privacy preferences of users. A privacy proxy which sits somewhere on the Internet does the negotiation between the privacy policies of services and privacy preferences of users on behalf of the personal privacy assistant. *pawS* is designed with mechanisms that support the principles of notice, choice and consent, proximity and locality, and access and recourse. *pawS* supports the principle of notice by the use of beacons to announce privacy policies to users. Choice and consent are supported by negotiating disclosure according to the privacy preferences of users. Since privacy beacons announce privacy policies only to those users within their range, the principle of proximity and locality are supported. Finally, access and recourse are supported by the system's ability to store disclosure, negotiation and service records. Apart from the system being an experimental one, the major setback lies in its dependence on the fact that the privacy preferences of users are downloaded from a trusted third party. The absence of a common language of expressing privacy preferences in mobile computing makes it even more difficult for it to be effective. Scalability is also an issue especially in areas of high beacon density (e.g. central business districts). Another limitation of the *pawS* is its inability to support multiple privacy preferences. For example, in real life situations, the user's privacy preferences at a given time could be: "Do not disclose my location to Tesco Supermarket, but allow Woolworth to know and retain my location information for 30 minutes". If mobile computing systems are to support evolving social practices (Palen, 1999), then the *pawS* inspires mobile computing research to even greater heights by motivating further exploration of the above limitations.

Yamada & Kamioka (2005) have proposed an Encapsulated Mobile Agent-based Privacy Protection (EMAPP) which is similar to the notion of a *pawS* except that the personal privacy assistant is made up of a privacy proxy which in turn is an encapsulation of users' privacy preferences, personal data, and a mobile agent. This encapsulation is termed a *privacy capsule.* A

location-based service within a mobile computing environment has a service proxy which contains the privacy policy of the service as well as a mobile agent. The mobile agents handle privacy preference negotiation between the service and privacy proxies. EMAPP is built on the same privacy beacon principle of the *pawS*. They therefore have similar limitations, except that EMAPP has the advantage of preventing the copy and misuse of personal information once initial access is granted. Apart from the limitations in expressing privacy preferences and scalability, the use of mobile agents introduces performance overheads as a crucial research issue in EMAPP implementation.

The privacy control architectures mentioned above have largely been built to protect privacy based on widely accepted principles. The next section takes a look at some privacy protecting systems and how requirements for privacy protection are derived from OECD's fair information practices.

## 2.10 Principles of Privacy Protecting Systems

Privacy protecting systems rely on declarations and laws of data protection. The OECD's Fair Information Practices (FIP) contain a broad set of guidelines for controlling the use of personally identifiable information (OECD, 1980). Therefore, the significance of the use of these guidelines in abstracting requirements for privacy protection systems cannot be over-emphasised. In this section I discuss the derivation of these principles from the OECD's guidelines and provide an extension by looking at two principles of privacy protection in mobile computing: the principle of minimum asymmetry and approximate information flows.

### *2.10.1 Requirements from Privacy Principles*

Many countries have implemented data protection legislation to protect civil liberties since the OECD publication in 1980 of guidelines on the protection of privacy and transborder flows of personal data. Most of these laws are based on the OECD's fair information practices and form the basis for consumer privacy protection (see Table 2.3).

Table 2.3: Privacy Principles from the Fair Information Practices

| **Principle** | **Description** |
|---|---|
| 1. Collection limitation | Data collectors should only collect information that is necessary, and should do so by lawful and fair means, i.e., with the knowledge or consent of the data subject. |
| 2. Data quality | The collected data should be kept up-to-date and stored only as long as it is relevant. |
| 3. Purpose specification | The purpose for which data is collected should be specified (and announced) ahead of the data collection. |
| 4. Use limitation | Personal data should only be used for the stated purpose, except with the data subject's consent or as required by law. |
| 5. Security safeguards | Reasonable security safeguards should protect collected data from unauthorized access, use, modification, or disclosure. |
| 6. Openness | It should be possible for data subjects to learn about the data controller's identity, and how to get in touch with him. |
| 7. Individual participation | Data subjects should be able to query data controllers whether or not their personal information has been stored, and, if possible, challenge (i.e., erase, rectify, or amend) this data. |
| 8. Accountability | Data controllers should be accountable for complying with these principles. |

The nature of mobile computing technologies described earlier suggests that it is not sufficient to derive privacy policies only from the above principles so as to protect the privacy of data owners. Jiang et al (2002) propose the principles of minimum asymmetry and approximate information flows which can be used as a basis for deriving additional privacy policies for mobile computing applications as well as LBS providers. The next section discusses these principles in detail.

### *2.10.2 Deriving privacy principles in mobile computing from the principles of minimum asymmetry and approximate information flows*

Jiang et al (2002) propose a principle of minimum asymmetry which reduces an imbalance of information flow between different parties taking part in data collection in mobile computing. The basis of this according to them is by seeing privacy as being about information flow control, in which a party involved in the use of the information has more information than the other (a condition often termed externality). The idea of externality was originally used by economists to describe connections, effects, and relations that are not considered in the course of a transaction (Ellis & Fellner, 1943; Jiang et al., 2002). This could be explained in a situation where an individual's personal information is collected by a service provider for the sole purpose of providing a particular service, eventually leading to the second use of such information by other third parties without the consent of the data owner. In this case, the data owner has little information of who uses their data, and for what purpose. Such a situation according to Jiang et al (2002), leads to negative externality usually imposing a burden on people without their consent.

The proposed principle of minimum asymmetry does not seek to solve privacy problems technologically, but applied as a design goal in mobile computing, addressing the other three forces (markets, norms, and legislation) according to Lessig (1998). The authors also proposed an approximate information flows (AIF) model that describes the flow of information involving various actors in three abstractions, namely, *storage*, *data flow*, and *end-user* perspectives. By approximating the flow of information and minimizing asymmetry, their proposed model suggests new privacy solutions that are socially-compatible, among other things.
Minimum asymmetry is achieved by:

1. *Decreasing the flow of information from data owners to data collectors and users,*
2. *Increasing the flow of information from data collectors and users back to data owners.*

Minimum asymmetry can be achieved by such methods as; anonymising and pseudonymising, increasing the granularity of location data, increasing the rate at which location information is sent back to the server, among other things. Any method that can be used to decrease the flow of information to achieve minimum asymmetry is termed noise as described in Section 2.11 below.

Three privacy-sensitive properties can be abstracted from the above principles. These are, *persistence of data* (from which we derive the notion of *retention time of data*), *accuracy of data* (which includes introduction of *noise*), and the *confidence of data* (uncertainty of data). Whilst persistence and accuracy of data can be applied to identity, location, and other contextual information, the uncertainty of data is usually useful in the capability of a particular technology in determining location information (e.g. the percentage certainty of sensors in determining a user's location, as against that for a GPS device).
Table 2.4 provides an extension of the principles listed in Table 2.3.

Table 2.4: Additional Properties for privacy policy derivation in mobile computing

| ***Property*** | ***Description*** |
|---|---|
| Location data rate of update | This is the rate at which data about the location of the user and/or device is updated on a central server |
| Retention time | The lifetime of the data e.g. users can set the location information they have used for a coffee shop finder to persist for just 5 minutes, preventing others from using such information later. |
| Accuracy of data (Introduction of Noise) | Preventing the true meaning of the data from being revealed Examples include: Anonymity, cloaking, blurring, hashing, and lying (deception) |

## 2.11 Comparison of Privacy Protecting Models in Mobile computing

Previous work aimed at helping mobile computing users protect their privacy, which generally means their location privacy, can be divided roughly into two groups:

1. *policy matching*: attempts to provide mechanisms for comparing a user's policy to that of the mobile computing service and notifies the user of mismatches, and;
2. *noise*: tries to hide or disguise a user's location or identity.

*Noise* is metaphorically defined as the intentional, or unintentional, manipulation or transformation of data preventing the true information in the data from being revealed. Noise includes, cloaking, blurring, anonymity (or pseudonymity), hashing or encryption, and lying (which I term benign deception). Noise can be divided into five types, namely:

1. *anonymising*: hiding the identity of the user;
2. *hashing*: disguising the identity of the user
3. *cloaking*: defined by Gruteser and Grunwald (2003) as the reduction in the spatial and temporal resolution of location information (i.e. *location cloaking)*.
4. *blurring*: decreasing the accuracy of the location (and possibly time); and
5. *lying*: giving intentionally false information about location or time.

Table 2.5 describes some research efforts in line with the above classification and how each is seen in the context of Jiang et al's classification (2002) and work on the extension of private data classification (Price et al., 2005). As evidenced from the table, substantial amount of work has been carried out in anonymising (Wu et al, 2008; Beresford & Stajano, 2003; Gruteser & Grunwald, 2003); blurring (Dunne et all, (2008); Duckham & Kulik, 2005; Gruteser & Grunwald, 2003); cloaking (Wu et al, 2008; AT&T, 2004; Gruteser & Grunwald, 2003; Hong & Landay, 2004); and hashing/encryption (Beresford & Stajano, 2003; Jorns & Bessler, 2004). The classification is done according to whether the type of privacy protection is preventive, avoidance, or detection rather than the classification by Ackerman (2004) for the sake of convenience.

Table 2.5: Comparison of Privacy Protecting Models in Mobile computing

| ***Author(s)/System Name*** | ***Description*** | ***Type of privacy protection*** | ***Method of protecting privacy*** |
|---|---|---|---|
| 1. ( Dunne et al, 2008;Duckham & Kulik, 2005) | Location blurring to nearby point | Preventive | Noise (Blurring) |
| 2. (Gruteser & Grunwald, 2003) | k-anonymity | Preventive | Noise (Blurring/Anonymity) |
| 3. (Beresford & Stajano, 2003) | Provides unlinkability between pseudonyms | Preventive | Noise (hashing) |
| 4. (Hong & Landay, 2004) **Confab** | Privacy proxy handles digitally signed privacy metadata | Avoidance, Preventative | Matching Policies, Noise(Cloaking, Lying) |
| 5. (Langheinrich, 2002) **Privacy Awareness System (pawS)** | Use of :<br>• privacy proxy<br>• privacy-aware database | Avoidance, Preventive | Matching policies |
| 6. (Gunter, Carl A. et al., 2004) **AdLoc** | Combining formal access control with PDRM (Personal Digital Rights Management) | Avoidance, Preventive | Matching policies/access control |
| 7. (Jiang et al., 2002) | Model:<br>• Approximate Information Flows<br>• The Principle of Minimum Asymmetry | Prevention, Avoidance & Detection | Detection, Feedback, Noise (Anonymity) |
| 8. (Lederer et al., 2002) | User Interface Metaphor: Situational faces metaphor – conceptualising end-user privacy preferences | Preventive | Matching Policies |
| 9. (Wu et al, 2008; AT&T, 2004) **Find People Nearby** | Node anonymity in mobile ad hoc netwokrs; friend finding application by AT&T | Preventive | Noise (cloaking) |
| 10. (Nguyen & Mynatt, 2002) **Privacy Mirror** | UI Metaphor: Privacy Interface (for feedback and detection) | Detection | Feedback |

Since the literature contains a substantial amount of work in the above techniques, I shall limit the scope of this thesis to techniques that represent established social practices and which present further research challenges in mobile computing.

## 2.12 Deception in Location Disclosure as a Privacy Control Mechanism

In this section, I define deception and discuss the moral and religious justification of its use in our study. Section 2.12.1 describes the legal and religious viewpoints about various forms of deception, whilst Section 2.13 discusses a number of deception implementations in mobile computing.

### *2.12.1 Deception*

The Oxford online reference dictionary of law defines deception as a *false representation, by words or conduct, of a matter of fact (including the existence of an intention) or law that is made deliberately or recklessly to another person* (Oxford Dictionary of Law, 2002). The same reference asserts that deception itself is not a crime, but becomes an imprisonable crime when it is involved in:

1. Obtaining property.
2. Obtaining an overdraft, an insurance policy, an annuity contract, or the opportunity to earn money (or more money) in a job or to win money by betting. These two offences are punishable by up to ten years' imprisonment.
3. Obtaining any services (e.g. of a driver or typist or the hiring of a car).
4. Causing someone to wait for or forego a debt owing to him.
5. Securing the remission of all or part of an existing liability to make payment (whether one's own or another's) with intent to make permanent default in whole or in part.
6. Obtaining an exemption from or abatement of liability to pay for something (e.g. obtaining free or cheap travel by falsely pretending to be a senior citizen).

However, it is not an offence "to deceive someone in any other circumstances, provided there is no element of forgery or false accounting" (Oxford Dictionary of Law, 2002).

Deception is not only an issue for legal discourse, but also an issue of grave concern to moral philosophers. Often synonymous to lying (the art of telling a lie), deception is seen to be morally wrong, though research shows its ethical justification in fields like medical ethics[1] (Bok, 1978). For instance, Maximus of Tyre says "A physician deceives a sick man, a general deceives his army and a pilot the sailors; and in such deception, there is no wrong." Prochus comments in Plato (360 B.C.E.): "For that which is good is better than the truth."

Since the beginning of ethical speculation, two opinions about deception or lying have always surfaced. While Aristotle (350 BC) in his work *Ethics,* contends that it is never permissible to lie, Plato (360 B.C.E.) in his *Republic* is more flexible in allowing lying by Medical Doctors and Statesmen to lie sometimes for the good of their patients and citizens respectively (Knight, 2003).

Religion has always played its part whenever morality is mentioned. Islam for instance, mentions some forms of acceptable deception. The Islamic concept of deception is called *Taqiya* and is defined by the Oxford Dictionary of Islam as a "precautionary denial of religious belief in the face of potential persecution (Taqiya, 2003). Stressed by Shi'a Muslims, who have been subject to

[1] pages 182 - 202

periodic persecution by the Sunni majority. The concept is based on *Quran* 3:28 and 16:106 as well as hadith, tafsir literature, and juridical commentaries."

According to (TheFreeDictionary.com) *Taqiya* is part shi'a Islamic tradition originating from as far back as the days when shi'as were a minority and used to be persecuted by sunnis. The Shi'as were usually forced to curse the house of Imam Ali by Sunnis, knowing that it was the last thing a devout Shi'a will do. Under such circumstances, the concept of *Taqiya* emerged allowing Shi'as to lie about their belief when they thought their lives were in danger so long as they held faith true in their hearts. This then brings us to the notion of *intention to lie*. One of the early works on this was by St Augustine. St Augustine's work is perhaps one of the most comprehensive discussions of deception from the moral point of view.

During the days of St Augustine (Augustine, 1952, 1961), certain deliberately deceptive statements were not considered as lies but deemed to be used in good conscience[2]. St Augustine described 8 kinds of lies as pertaining to:

1. Religious doctrine

A lie:

2. that profits no one and injures someone
3. that profits one party so as to injure another
4. told out of mere lust of lying or deceiving
5. told out of the desire to please
6. that injures no one, and profits someone in saving his money, for example.
7. that injures no one and profits someone in saving him from death
8. injures no one and profits someone in saving him from defilement of the body

In *Summa Theologica* Thomas Aquinas (1947) having regarded St Augustine's classification as insufficient in the 13th Century, distinguished 3 kinds of lies as **officious** (often told for useful purposes); **jocose** (told for fun); and **mischievous** lies (usually told to harm someone). Aquinas agreed that only the 3rd lie constituted a mortal sin whilst officious and jocose lies were less serious. The pattern of lies as described in the *Summa Theologica* is still being followed by catholic theologians today[3] (Bok, 1978).

Immanuel Kant[4] "on a supposed right to lie for altruistic motives" summed up his belief as follows: "To tell the truth is a duty, but it is a duty only toward one who has a right to the truth." This section has provided some background to different viewpoints of deception and demonstrates its

[2] page 35

[3] page 34

[4] page 267

moral justification in various circumstances. The exposition is necessary because it provides a moral and ethical basis for the re-contextualisation of deception from other disciplines to the field of mobile computing.

## 2.13 Deception and Mobile Computing Privacy

A number of research efforts in mobile computing have attempted to address the notion of deception. Benford et al (2004) use "self-reported positioning" to disclose the location of players of a location-based game, "Uncle Roy All around You", using an electronic map. In this game, players can lie about their location in order to rendezvous with Uncle Roy, an elusive character, as they move round a 3D model of a city. This is perhaps one of the first known location-based systems to implement the notion of deception in location disclosure. However, since the method of self-reported positioning has been successfully applied only to location-based games, I argue that a lot more needs to be investigated in terms of location-based services in general. For instance, in real world settings users usually have many and/or different privacy preferences at a time: *reveal my actual location to "A"; send a coarse granularity location to service "B",* etc.

Duckham & Kulik (2005) describe a formal model for an intentional degradation of the quality of information in order to protect the location privacy of the owners of such information, a process termed *obfuscation.* Their work focuses on the use of imperfection in spatial information to obfuscate location information. Three types of imperfection can be identified in the literature: *inaccuracy, imprecision, and vagueness,* in which inaccuracy describes the absence of correspondence between information and reality; imprecision is the inability of information to describe specifics; and vagueness is described as the existence of *boundary cases* in information (Duckham & Kulik, 2005; Duckham et al., 2001; Worboys & Clementini, 2001; Worboys & Duckham, 2004). The obfuscation model provides a mechanism of balancing location privacy with a high quality of location-based service. However, no explicit attempt to completely introduce deception into the model has been made. The model at this stage merely implements imprecision to protect location privacy.

A more advanced form of deception in location disclosure was recently developed by Iachello et al (2005). Iachello and his colleagues carried out quite an extensive study on a social network of 11 participants to measure the occurrence of deception in the form of *delayed answers* (i.e. the user intentionally delays answering a location request); *time-shifted answers* (in which the user responds with a past or future location); *ignored requests;* and *explicit deception* (i.e. responding with an intentionally inaccurate location disclosure). Though not explicitly stated, the study assumes a social network to be a network of person to person interactions. However, the definition of a social network by (Papakyriazis & Boudourides, 2001) broadens the scope of a social network to include

individual people, groups of people, objects or events "as far as certain relations hold them together". More so, the mode of deception implemented is manual-based, making it difficult for users to handle multiple *deception preferences* for waypoints and instant reply lists. Deception preferences are the options users have on how deception should be implemented during location disclosure. Examples include one-time deception (e.g. deceive this person about my location just this once), specific-time deception (e.g. allow automatic deception when my boss requests for my location every working day after 5pm), manual deception (always ask me to manually choose the location to use in implementing deception), etc. Furthermore, the study carried out by Iachello and his colleagues was mainly based on responses from an Experience Sampling Method (ESM) survey without consciously considering the reduction in dissonance that exists between the privacy attitudes and behaviours of participants.

### *2.13.1 Summary*

In this chapter, I have progressively articulated from the literature how location privacy poses a research problem in social mobile computing. I have also provided an exploratory study into the justification of the use of deception in areas such as medical ethics and religion. Deception as has been described can be controversial depending on the context of its use. Research in social psychology has shown that deception is essential for protecting environmental privacy (i.e. the right to be left alone) (DePaulo & Kashy, 1998; Hancock et al., 2004). However, if technology is to cope with social norms, then the justification of the use of deception from the moral philosophy viewpoint needs to be clarified. There is already ample proof that deception may have positive benefits to society as a whole. However, what is not certain is whether this whole concept is useful in controlling privacy in mobile computing. Better still, if even at all useful, the extent of this usefulness will be crucial in the design of privacy-sensitive architectures in mobile computing.

In the next chapter, I describe an exploratory study conducted to investigate the extent to which deception can be used to control location privacy. The study is based on scenarios designed to cater for various contexts of use of deception, including its use for good purposes, in establishing social harmony, and based on interactions within a social network setting.

# *Chapter 3. To What Extent Can Deception Control Location Privacy?*

## 3.1 Introduction

Evidence from my own interactions and from social psychology suggests that people will sometimes deliberately withhold their location information to protect their privacy, among other reasons. However, there is the need to further explore empirically the extent to which this kind of deception can be extrapolated to the wider population and under what circumstances this will be acceptable.

I present three different scenarios describing some circumstances under which deception can occur. Each scenario investigates the level of uneasiness participants feel by engaging in deception as well as how likely they will deceive when queried about their location. In order to determine the validity and effectiveness of responses from this study, each scenario is designed to include location requests coming from a spouse or partner, a parent (if any), their child(ren) (if any), a workplace boss, a colleague, a friend, other family member, and a stranger. For the purpose of this work, I call the group of these requestors the discloser's social network.

During the study (which was online based) participants were initially asked more general questions involving location disclosure for requests coming from each member of the social network. They were then taken through a set of questions involving the likelihood of sending an untrue location and the level of discomfort in making such a disclosure.

## 3.2 Scenarios

Scenarios present a powerful way of exposing a design to critique (Carroll, 2000). According to Carroll scenarios are stories about people and their activities. Scenarios "*highlight goals suggested by the appearance and behavior of the system, what people try to do with the system, what*

*procedures are adopted, not adopted, carried out successfully or erroneously, and what interpretations people make of what happens to them.*" (Carroll, 2000). Scenarios "*evoke reflection-in-action*" (Schon, 1983).

Figure 3.2-1 describes Carroll's five reasons for the use of scenarios for design. Scenarios address five key design challenges. The outer part of the scenario-based design pentagon represents these challenges, whereas the role scenarios play in addressing those challenges is illustrated in the body of the pentagon.

My choice of employing scenarios in this research is underpinned by the very same reasons outlined by Carroll, especially, the use of scenarios to evoke reflection in designs. This is because with the flexibility that comes with scenarios, it is much easier to carefully design good scenarios that will not only capture the key design considerations but also help in evoking the right kind of reflection in action. Other options that could have been employed include the use of case studies. However, with the relatively limited use of location-based services by the general public, very few case studies if at all existent, will serve this purpose.

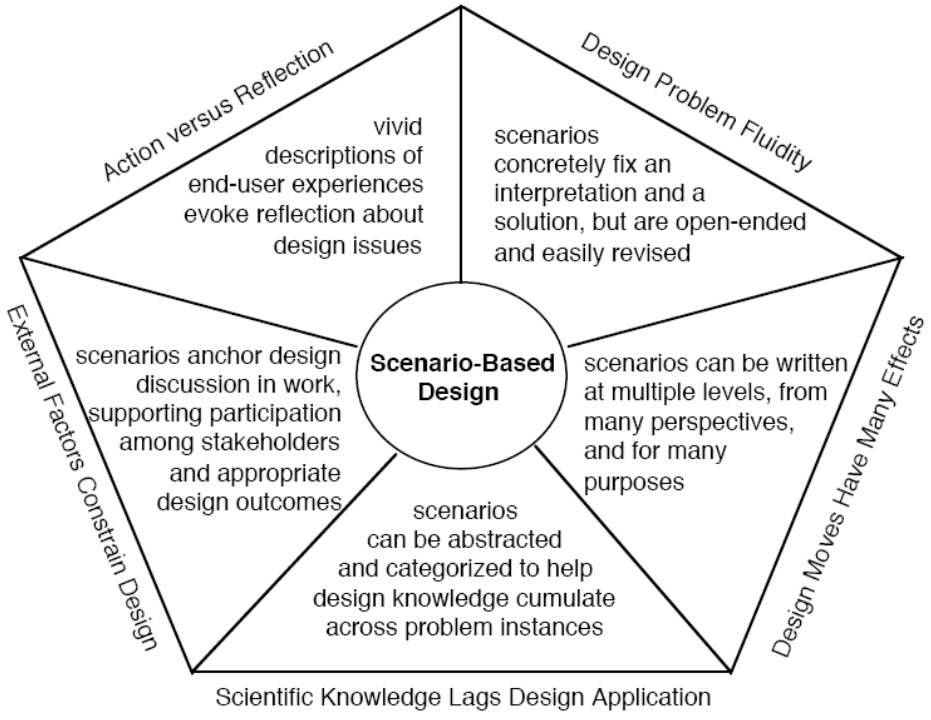


**Figure 3.2-1: Reasons for Scenario-based Design (Carroll, 2000)**

## 3.3 Study Objectives

The objective of this study was to investigate the feasibility and acceptability of the use of deception to protect location privacy by:

a. using scenarios to gather data. The scenarios employed in this study include *the use of deception for good purposes; the use of deception to preserve or enhance social harmony; and the use of deception in circumstances other than for good intentions or preserving social harmony.*
b. exploring the general acceptability of the use of deception in each of the above scenarios.
c. finding out limitations for the use of deception in each of the above three scenarios.

Key goal indicators for this study include:

1. The likelihood of the use of deception across the above three scenarios.
2. The level of discomfort expressed after engaging in deception across the above three scenarios. Discomfort in this study is defined *as the uneasiness experienced by participants when they have disclosed an untrue location*.
3. The percentage of study participants who will engage in deception or forms of it to protect their privacy.

The advantage of the use of scenarios is that it is possible to carry out studies on systems that are yet to be developed (Lederer et al., 2003). The low cost expense in the use of online scenarios makes it popular among researchers in this area.

However, scenarios come with a price to pay if they are not well structured to prevent study participants from misunderstanding what they try to illustrate. Secondly, such studies run the risk of getting results that may be in cognitive dissonance, where participants' actual behaviour may be different from their stated preferences (Lederer et al., 2003).

## 3.4 Preliminary Study

The study was conducted in two stages. Initial data collection was done with participants drawn from an email sent to staff and students of the faculty of Maths and Computing of the Open University. The essence of the pilot study was to help identify any questionnaire design issues as well as potential technical setbacks that might have an impact on the study. The pilot study took one week to complete. As the design was based on The Open University's Elsa[5] survey system, I had no significant questionnaire design layout issues during the pilot stage, paving the way for the real study. The only issues recorded had to do with clear, concise and meaningful questionnaire construction.

[5] http://elsa.open.ac.uk

## 3.5 Method

### 3.5.1 Participants

Study participants were 394 members of a research panel of Open University (OU) students called 'PRESTO'. The PRESTO panel is representative of the entire OU population of students. However, the average age is slightly older than the average student age in the United Kingdom. The PRESTO panel consists of OU students who have volunteered to take part in online research surveys conducted by staff of the University. The group was chosen for two reasons. Firstly, this panel had been taking part in similar surveys (e.g. the privacy and self-disclosure online project - http://www.york.ac.uk/res/e-society/projects/15.htm) and therefore, it was not difficult to reach them via one email. Secondly, the demographic distribution of participants in the PRESTO panel (consisting of the 18 – 90 year age range across the whole of the United Kingdom, in the case of this study) makes them a unique group of people to participate in large scale studies of this nature. Participants did not have go through the trouble of filling forms to opt in. They were part of a dedicated pool of study participants in the Open University who had accepted to take part in such studies. Therefore emails were sent out to the pool with permission from the moderator. Out of 682 emails that were sent out to potential participants via The Open University's *Elsa* system, 394 read the introduction. A total of 382 either finished one or more complete scenarios, representing 96.95% of all those who attempted the study.

An initial response rate of 60.43% was achieved in this study, but after responses that did not provide results for a complete scenario were removed, the final response rate was 58.59%.

Of the 394 participants, 45% (178) were male, 53% (209) were female, whilst 2% (8) had no demographics available. The mean age of the sample was 43.3 years, (range: 18 – 90 years, SD = 10.55). A total of 1774 responses were recorded during the study as shown in Table 3.1 below and captured by the *Elsa* system.

**Table 3.1: Breakdown of Overall Participation**

| | Number | Percentage of all approached | Percentage of all available |
|---|---|---|---|
| Participants Approached via Email | **682** | **-** | **-** |
| Bounced Back Emails | **27** | **3.96%** | **-** |
| Participants Opting Out | **3** | **0.46%** | **-** |
| Total No. of Participants available | **652** | **95.6%** | **-** |
| Available Participants Who Began the study | **394** | **57.78%** | **60.43%** |
| Participants Who Completed 1 or More Scenarios/Sub-studies | **382** | **56.01%** | **58.59%** |

### *3.5.2 Materials*

Since this study was web-based, the only item needed for each study participant was a computer with internet access. Data collection and analysis was straightforward with the Elsa system as it has an in-built capacity to collect raw survey data in any format defined by a study.

### *3.5.3 Procedure*

The study was divided into four parts, namely, (i) *general location disclosure methods, (ii) disclosure of an untrue location for good purposes, (iii) disclosure of an untrue location to maintain social harmony, (iv) disclosure of an untrue location for reasons other than the above.* I chose not to limit the last scenario (in (*iv)* above) to a specific one such as "for a bad reason" because I wanted to make the options open to participants, in order to further investigate what other forms of deception could potentially be useful for investigation, for reasons other than for good purposes or to preserve or enhance social harmony.

The general procedure for each part is presented in the following sections. The questionnaires used are reproduced in Appendix A.

#### 3.5.3.1 General Disclosure

In this section of the study, participants were presented with eight questions each, pertaining to how they would in general disclose their location to a stranger, their child(ren), a parent, a friend, a spouse or partner, a workplace colleague, or a boss at work. They were presented with different location disclosure methods to select from. These included: (i) always provide exact location; (ii) give false location information; (iii) vary the precision of location (iv) ignore location request; and (v) other methods of disclosure. Details of this can be found in Appendix A. The percentage of participants responding to each question is shown in Table 3.3. Section 3.6 below presents an analysis of responses recorded for this part of the study.

#### 3.5.3.2 Disclosure of an untrue location with a good intention

This section of the study was divided into two parts, with each part containing seven sets of questions. On one part, participants were asked how likely they were to disclose a false location to each of the following: their child(ren), a parent, a friend, a spouse or partner, a workplace colleague, or a boss at work. A scale of 1 to 5 was used to score each response. "1" represents a "very likely" response to each question. "5" represents a "not at all likely" response. Appendix A

Section B shows the study in detail. Table 3.4 and Figure 3.6-2 below show the mean responses for each question. An analysis of this is also provided in Section 3.6.2.

In the second part of this study, participants were asked how comfortable they were in disclosing a false location to each person presented in the first part of the study (if even with a good intention), namely: their child(ren), a parent, a friend, a spouse or partner, a workplace colleague, or a boss at work. A scale of 1 to 5 was used to score each response, with "1" representing "very comfortable" and "5" representing "not at all comfortable". In order to express this range of comfort in a consistent way across my results, I use the term discomfort as the base expression and have mapped these to a score of "1" representing a low level of discomfort (as per the definition of discomfort in Section 3.3), whereas a score of "5" represents a high level of discomfort. This less formal definition of comfort/discomfort and the subsequent analysis is intended to examine the possible impediments to use of the techniques to protect privacy (with specific emphasis on location). Table 3.4 shows the mean level of discomfort recorded for each question by all participants. An analysis of this is described in Section 3.6.2.2.

#### 3.5.3.3 Disclosure of an untrue location to maintain social harmony.

This is similar to the previous section, except that the purpose for a false disclosure is different. In this case participants were told that the reason for disclosing a false location was to maintain social harmony, e.g. in situations where one is running late to meet a friend, colleague, boss, parent, child, spouse or partner, or other family member, but does not want them to know they still have not set off yet. The scores for likelihood and level of discomfort were captured and recorded in the same way as the previous section.

#### 3.5.3.4 Disclosure of an untrue location for reasons other than the above

This part of the study was conducted in the same way as in Sections 3.5.3.2 and 3.5.3.3 above. However, participants were to think of reasons for an untrue location disclosure other than for a good purpose or to maintain social harmony. The scores were captured and recorded in the same way as described above. Analysis of this is found in Section 3.6.3.3 below.

## 3.6 Results, Data Analysis and Findings

In this section, we present results of each part of the study and analysis of the findings. Table 3.2 below presents a breakdown of the responses provided for each scenario or section of the study.

**Table 3.2: Breakdown of Responses by Scenarios**

| Study/Scenario | No. of responses |
|---|---|
| General Disclosure | 382 |
| Deception for Good Intentions | 361 |
| Factors Influencing Plausible Disclosure | 337 |
| Deception to Enhance Social Harmony | 353 |
| Deception for Other Purposes | 341 |
| | **Total: 1774** |

### *3.6.1 Investigating how location is disclosed in general to a requestor*

Participants were asked how they thought they would disclose their location to requests coming from people within their social networks in circumstances where it would be in no way embarrassing to reveal their location. The following sections describe the results obtained for requests coming from each person within their social network.

**Table 3.3: Response Rate for General Strategies in Making Location Disclosures**

| | **Requestor** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Spouse/Partner** | **Friend** | **Colleague** | **Workplace Boss** | **Parent** | **Child** | **Other Family** | **Stranger** |
| **Always provide exact location** | 80.1% | 39.7% | 35.3% | 29.5% | 52.8% | 77.3% | 45.3% | 1.1% |
| **Give false location** | 0.5% | 0.5% | 0.3% | 1.6% | 2.5% | 0.8% | 0.5% | 5.3% |
| **Blurring** | 13% | 46.1% | 43% | 40.7% | 21.6% | 15.6% | 43.9% | 10.1% |
| **Ignore request** | 4% | 10.2% | 17.8% | 22% | 10.1% | 3.4% | 7.3% | 79% |
| **Other strategy** | 2.4% | 3.5% | 3.7% | 6.2% | 13.1% | 2.8% | 3% | 4.5% |

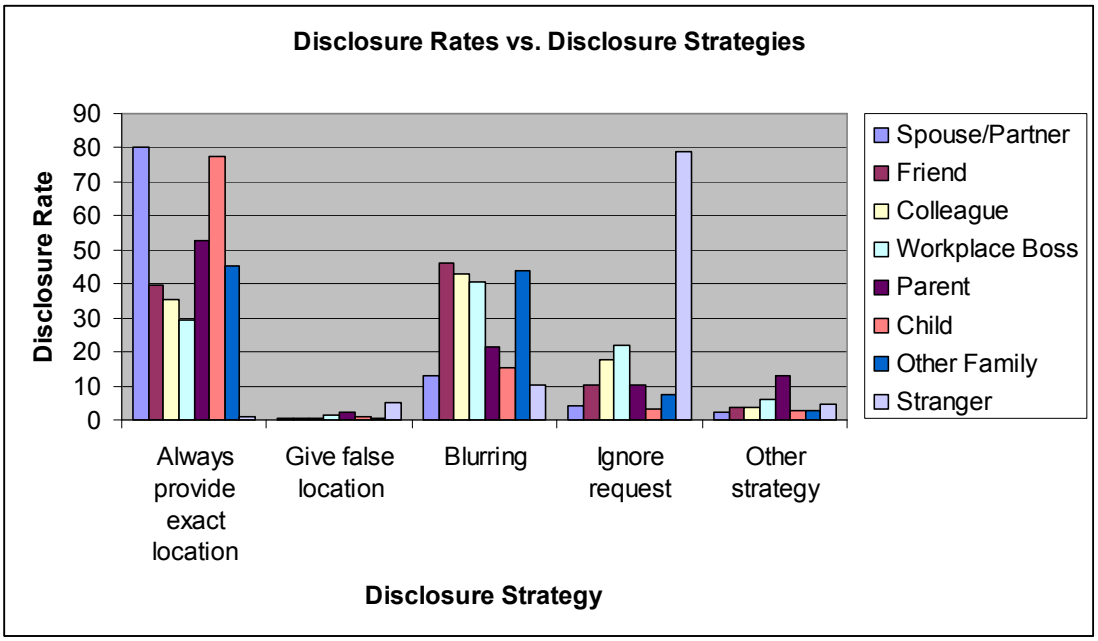


**Figure 3.6-1: Perception of the Use of Disclosure Strategies for Requests Coming from Each Member of the Discloser's Social Network**

#### 3.6.1.1 Disclosure Method: Always Provide Exact Location

In general, most participants will disclose their exact location to requests coming from their immediate family members within their social network. 80.1% will disclose their exact location to a spouse or partner, 77.3% will disclose to a request coming from their children, 52.8% from their parents, and 45.3% to other family members. In contrast, less than 40% will disclose their exact location to a friend, workplace colleague, boss, or a stranger (representing 39.7%, 35.3%, 29.5%, 1.1% respectively).

#### 3.6.1.2 Disclosure Method: Provide False Location

Explicitly disclosing false location information scored the lowest disclosure rate (from 0.5% to 5.3%). 5.3% will disclose a completely false location to a request coming from a stranger or someone they did not know.

#### 3.6.1.3 Disclosure Method: Varying the precision of location (Blurring)

A small percentage of participants (13%) will intentionally blur their location before disclosing it to their spouses or partners. Blurring as a technique of withholding location information was popular with requests coming from friends, workplace colleagues, bosses, and other family members (representing 46.1%, 43%, 40.7% and 43.9% respectively).

#### 3.6.1.4 Disclosure Method: Ignoring Location Request

Though some participants will ignore requests coming from the rest of the members of their social network, a high percentage (79%) will completely ignore requests coming from strangers or people they did not know.

#### 3.6.1.5 Disclosure Method: Other Strategies

Fairly low disclosure rates were recorded for other strategies not explicitly included in this study. These strategies range from generic excuses (network busy, etc) to switching off one's phone. Only requests coming from parents recorded a rate above 10% (i.e. 13%), followed by requests coming from a workplace boss (6.2%).

### *3.6.2 Withholding Location Information for Good Purposes*

As has been described in Chapter 2 Section 2.12.1, some forms of deception are seen to be engaged in with good intentions. Examples of such forms of deception with specific reference to location disclosure include the following scenarios.

*You are in a gift shop about to buy a present for a loved one. Disclosing your true location to the recipient of the present is likely to give them an indication of the activity in the shop.* Therefore, when requested for one's location by the recipient of the gift at the time of buying the gift, I describe the disclosure of an untrue location in this case as deception for good purposes. Hence, I classify the deliberate disclosure of a false location in less harmful situations (often called *white lies*) as deception for good purposes.

For each of the questions in this scenario, study participants were asked to imagine that they had mobile phones that were equipped with location sensing and disclosure functionality. They were further asked to imagine they were in a gift shop about to buy a surprise gift for a person, and that they had set their phones to reveal a different but plausible location to that person when they asked for their location.

**Table 3.4: Mean Likelihood and Level of Discomfort for the Disclosure of a False Location with a Good Intent**

| Requestor | Mean Likelihood (Range 1-High, 5-Low) | Mean Level of Discomfort (Range 1-Low, 5-High) |
|---|---|---|
| Spouse/Partner | 2.97 | 3.67 |
| Boss | 2.85 | 3.04 |
| Parent | 4.06 | 4.08 |
| Child | 3.89 | 4.15 |
| Colleague | 2.85 | 2.89 |
| Friend | 3.04 | 3.36 |
| Other Family | 3.03 | 3.34 |

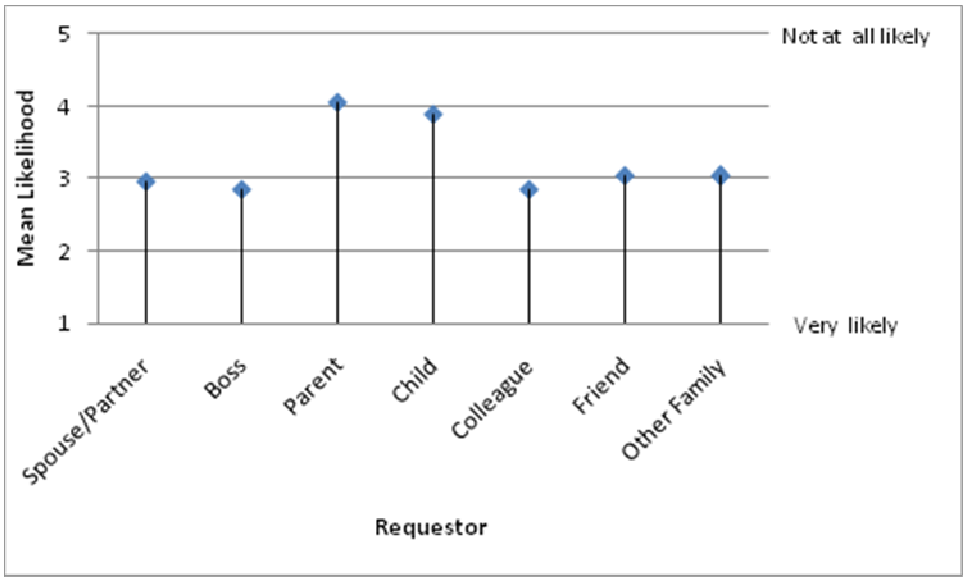


**Figure 3.6-2: Mean Likelihood of Disclosing a False Location with a Good Intent**

### 3.6.2.1 Likelihood of Disclosing a False Location for Good Intentions

Using a 1 to 5 scale corresponding respectively to *very likely* to *not at all likely*, the mean likelihoods are shown on Table 3-5 above.

The mean likelihood of disclosing a false location for good purposes is fairly constant (~3) for requests coming from a spouse/partner, workplace boss, workplace colleague, friend, and other family member. However, there was less likelihood to disclose a false location to a parent or child (~4).

The following quotes illustrate some of the opinions participants recorded regarding how they will disclose their locations with good intentions:

- *As it is with good intentions, I would feel it's more of a "white lie" than a serious deception, as it's to avoid spoiling the surprise.*
- *As long as giving false location wouldn't cause any problem or lead to any harmful situation*
- *I believe my location should only be available to close friends and family*
- *If buying a gift then I would always feel okay about giving a false location*

It is clear from the above comments that although participants had varied reasons for their responses, a clear pattern emerged from the study. That is, participants may disclose a false location to people in their social network, even to their parents or children.

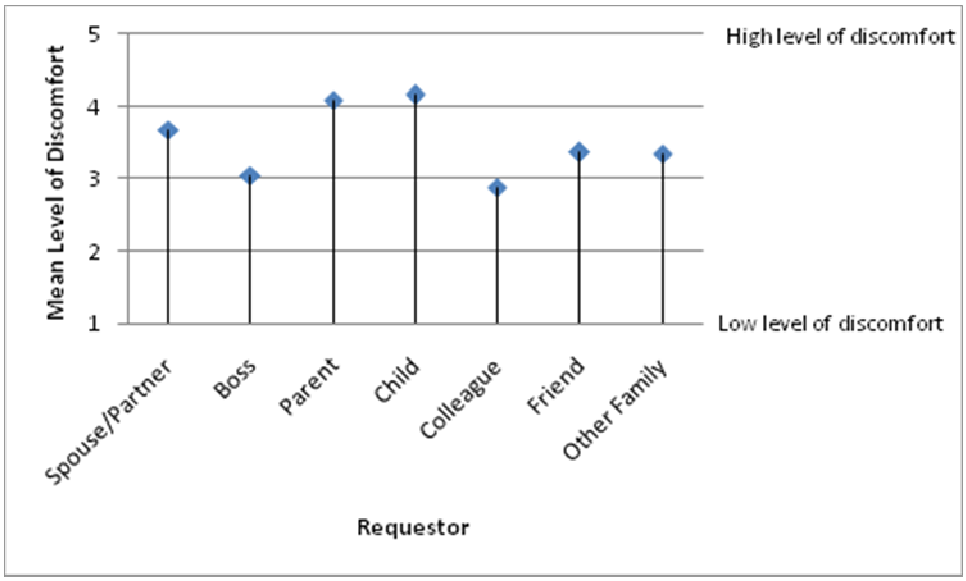


**Figure 3.6-3: Mean Level of Discomfort after Disclosing a False Location with a Good Intent**

3.6.2.2 Level of Discomfort after Disclosing a False Location for Good Intentions

A measure of the level of discomfort participants will have after disclosing a false location with a good intent gives an indication of how effective this kind of deception will be in protecting location privacy. On a scale of 1 (low level of discomfort) to 5 (very high level of discomfort), there was generally some level of discomfort in disclosing a false location to all members of the participants' social networks. The mean level of discomfort was high for requests coming from their parents or children (slightly above 4), echoed by the following comments from some of them:

- *Likelihood and comfort depend on the right of the person to know where I am. Child has highest right then wife, boss etc*

- *I am very comfortable about family and friends being able to track me, but uncomfortable about others being able to do so, except in an emergency and at my choosing*

- *I would only feel comfortable in any of these circumstances if it was for a good intention - anything else is just the same as lying, and I will happily lie to hide a good secret but not a bad one*

### *3.6.3 Deception as a Tool to Enhance Social Harmony*

Enhancing social harmony is one of the reasons why people sometimes engage in deceptive practices as outlined in Chapter 2, Section 2.12.1. Study participants were taken through two scenarios that describe the use of deception in enhancing social harmony. For example, if one is running late to meet a person and yet does not want him or her to know that they have still not left, then we say that disclosing a location other than the true location is done out of the desire to maintain existing social ties. For more details on this see Appendix A.

**Table 3.5: Mean Likelihood of Disclosing a False Location to Enhance Social Harmony**

| Requestor | Mean Likelihood (Range 1-High, 5-Low) | Mean Level of Discomfort (Range 1-Low, 5-High) |
|---|---|---|
| Spouse/Partner | 3.88 | 4.46 |
| Boss | 2.76 | 3.28 |
| Parent | 3.81 | 3.99 |
| Child | 4.5 | 4.71 |
| Colleague | 2.9 | 3.16 |
| Friend | 3.41 | 3.83 |
| Other Family | 3.56 | 3.91 |

#### 3.6.3.1 Likelihood of Disclosing a False Location to Enhance Social Harmony

Using the same scale of 1 to 5 (1 corresponding to *very likely* whilst 5 means *not at all likely*), the mean likelihood of disclosing an untrue location to maintain existing social harmony is shown in Figure 3.6-4 below.

The mean likelihood of disclosing a false location is about the same for requests coming from a spouse/partner or parent (~4). Requests coming from a friend or other family member are equally likely, though more likely than that for the spouse/partner or parent. However, the requestors having the most likelihood of receiving false disclosures in order to maintain social harmony are the workplace boss or workplace colleague. The requestor with the least likely to receive false disclosures for the sole purpose of maintaining social harmony is the child. This was not surprising, given the fact that the family relations between a parent and child far outweigh the other wise social relationship that may exist between them.

Therefore, in terms of the likelihood of maintaining existing social relationships or enhancing social harmony, the workplace boss and colleague, and a friend, are those that are most likely to receive false disclosures when a location request is made.

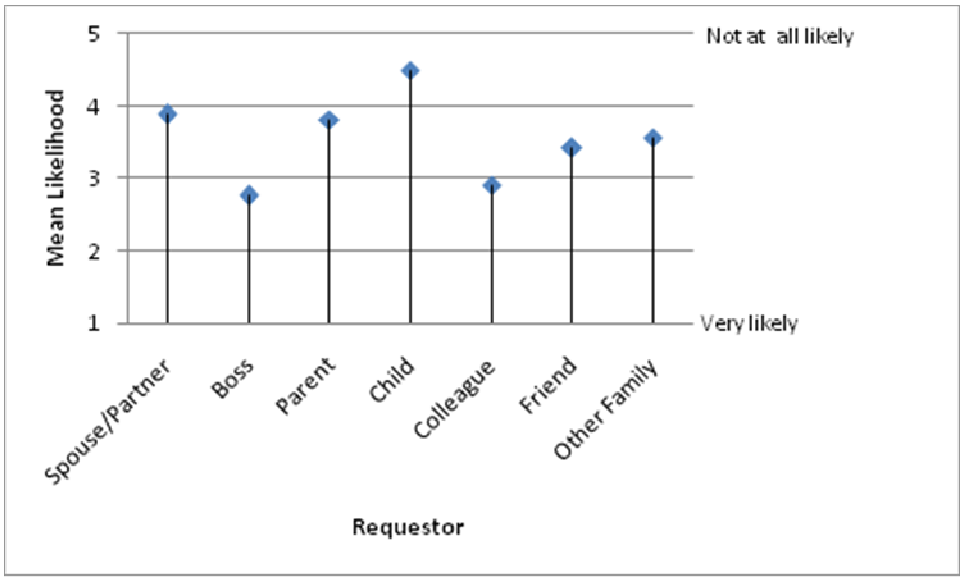


**Figure 3.6-4: Mean Likelihood of Disclosing a False Location to Enhance Social Harmony**

This is what one participant had to say regarding the disclosure of false location to enhance social harmony:

- *With people I am close to I would have no problem coming clean and admitting I'm running late or in an awkward situation and would expect them to be understanding and supportive. With people I'm less close to whereas I'm uncomfortable lying, whatever my situation is my business not theirs*

### 3.6.3.2 Level of Discomfort after Disclosing a False Location to Enhance Social Harmony

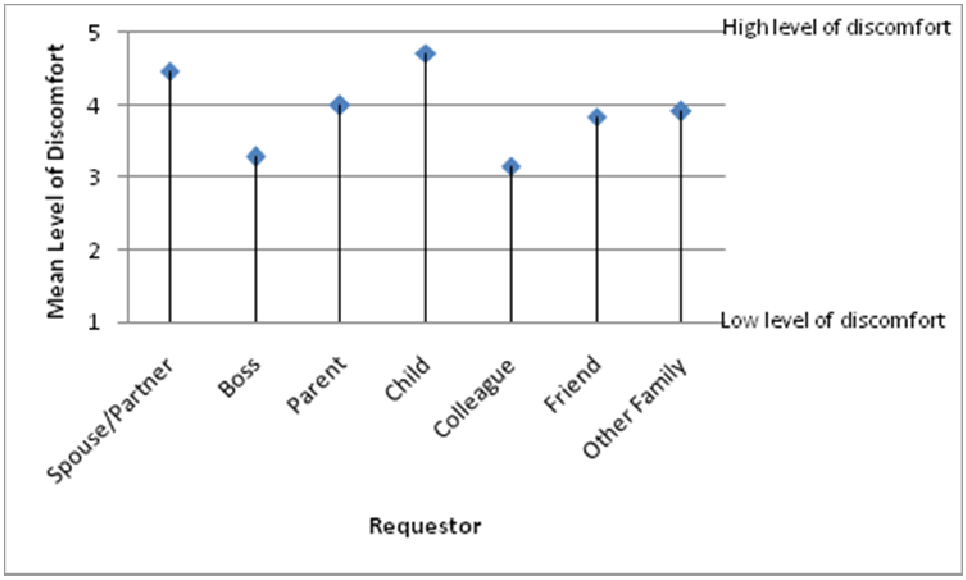


**Figure 3.6-5: Mean Level of Discomfort After Disclosing a False Location to Enhance Social Harmony**

There is a consistent pattern in the level of discomfort perceived from disclosing a false location to children. As in previous scenarios, the most discomfort comes from making false disclosures to children (4.71 in this case). However, the least discomfort comes from disclosing false locations to workplace colleagues and workplace bosses (representing 3.16 and 3.28 respectively), summed up in the following comments by a study participant:

- *I am afraid that I would not feel comfortable lying in the circumstances described above. It's a work thing. It would be very easy to lie to people indeed I am currently engaged in a running joke in work where some know the truth and others do not. This involves the fictitious purchase of a bottle of Grange wine from Sainsbury's at £109 approx and charging it to expenses. Obviously I have not done this but only 3 people know the truth and I am waiting to fictitiously pass the financial audit for my expense claim. A childish thing perhaps but it makes a change to the usual office banter. Perhaps it is the degree to which you can cause harm, hurt and distrust. My colleagues are used to far worse generally and will take it in good humour. Magicians deceive but perhaps stage hypnotists would score badly in the deceit and harm stakes. -*

#### 3.6.3.3 Deception in Other Scenarios

We categorise all scenarios other than ones with good intents or to enhance social harmony as *other scenarios.* Such scenarios could either stem from malicious intents, jocous purposes, or otherwise. For example, if one is in a location or engaged in an activity that they will feel embarrassed for a location requestor to know.

**Table 3.6: Mean Likelihood and Level of Discomfort of Disclosing a False Location in Other Scenarios**

| Requestor | Mean (Likelihood) | Mean (Level of Discomfort) |
|---|---|---|
| Spouse/Partner | 3.63 | 4.59 |
| Boss | 2.67 | 3.33 |
| Parent | 3.88 | 4.1 |
| Child | 3.7 | 4.69 |
| Colleague | 2.66 | 3.24 |
| Friend | 3.2 | 3.91 |
| Other Family | 3.09 | 3.89 |

#### 3.6.3.4 Likelihood of Disclosing a False Location for Other Scenarios

The mean likelihood of disclosing a false location in this type of scenario is about the same for requests coming from spouse/partner, parent and child (represented as 3.63, 3.88, and 3.70 respectively). The most likely scenario for the disclosure of a false location is the situation

where location requests come from a workplace boss or colleague (represented as 2.67 and 2.66 respectively). However, the perceived likelihood for disclosing a false location to a friend or other family member is almost the same, i.e. 3.2 and 3.09 respectively. The responses captured are further echoed by statements from study participants such as the following:

- *As before, willingness to deceive would depend on specific family member*
- *Why do these people need to know where I am - with the exception of the child - 24 hours a day?*

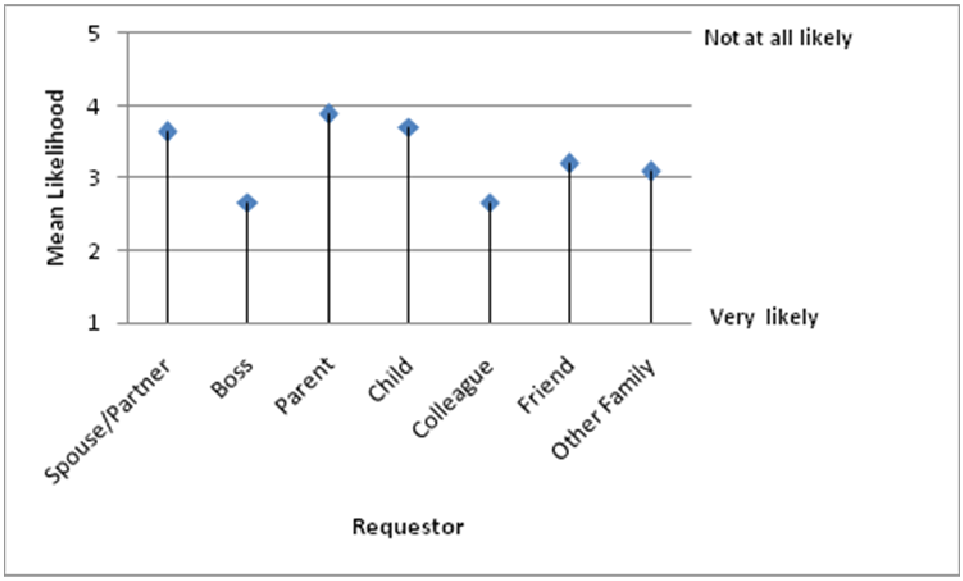


**Figure 3.6-6: Mean Likelihood of Disclosing a False Location for Other Scenarios**

3.6.3.5 Level of Discomfort after Disclosing a False Location for Other Scenarios

Requests coming from very close family ties (i.e. spouse/partner, parent, and child) register the highest discomfort levels (4.59, 4.10, and 4.69 respectively) than other members of the discloser's social network. As in other scenarios, the pattern of workplace boss and workplace colleagues registering the lowest discomfort levels (3.33 and 3.24 respectively in this scenario) confirms what a participant said in the following statement:

- *I would lie, but not feel comfortable about it to partner and family. To friends and colleagues, I would feel that it was not their business.*

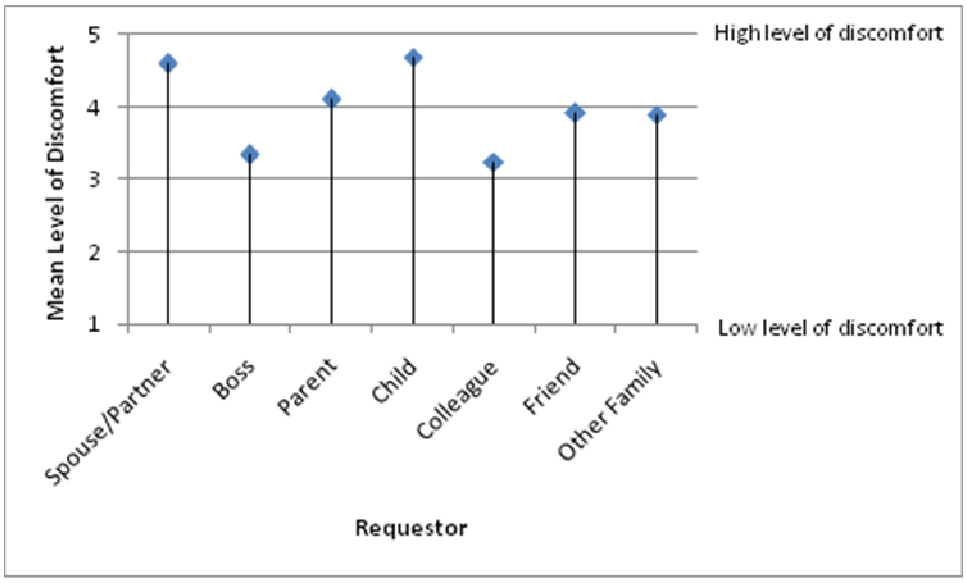


**Figure 3.6-7: Mean Level of Discomfort in Disclosing a False Location for Other Scenarios**

### *3.6.4 Comparison of Likelihood and Level of Discomfort across All Three Scenarios*

Figure 3.6-8 and Table 3-8 show that though participants indicated a likelihood of disclosing an untrue location in the particular circumstances described above, there was also some level of discomfort or uneasiness in doing so.

The possible reason for such a high level of discomfort across all three scenarios is investigated in Section 3.7

**Table 3.7: Summary of Mean Likelihood and Level of Discomfort Across All Three Scenarios**

| Scenario | Likelihood | | Level of Discomfort | |
|---|---|---|---|---|
| | Mean | SD | Mean | SD |
| Good Intention | 3.24 | 0.509 | 3.5 | 0.486 |
| Social Harmony | 3.54 | 0.598 | 3.91 | 0.565 |
| Other Scenarios | 3.26 | 0.492 | 3.96 | 0.559 |

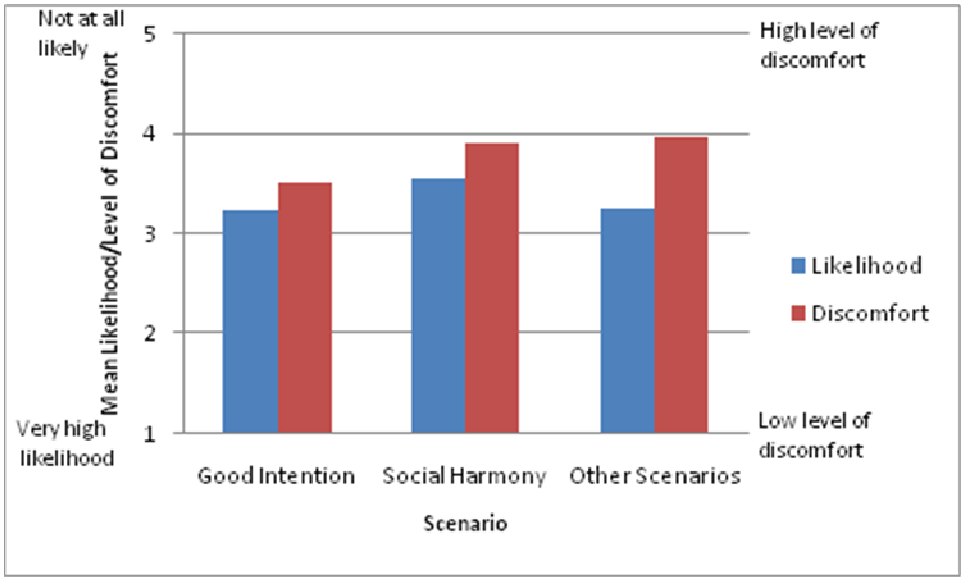


**Figure 3.6-8: Likelihood versus Level of Discomfort across Three Scenarios**

## 3.7 Causes of High Level of Discomfort in the Use of Deception to Protect Location Privacy

In the previous study in Sections 3.1 – 3.5 there was some level of discomfort across all scenarios. Could the discomfort be the result of a strong ethics opinion on the part of study participants? Did the participants' fear of being found out (after engaging in disclosing a false location) play a major role in the high level of discomfort? These questions are further explored in this section in which an online between subjects study was carried out to investigate the reasons for the high level of discomfort.

### *3.7.1 Method*

This follow on study had a different group of participants from the first study. Therefore in this section the method used in obtaining responses from study participants is described in detail.

#### 3.7.1.1 Participants

Study participants were drawn from The Open University's *Elsa* panel. In all an email was sent to approximately 900 people of which 503 valid responses were recorded. The same study protocol was used in this study as the first study described in Section 3.5.

#### 3.7.1.2 Materials

As in the previous study, the only requirement for this study was access to internet. The detailed contents of the study can be found in Appendix B. Participants did not have to fill in consent forms as they were recruited from the Open University panel of study participants, who had signed up to be used for such purposes as and when they arise.

#### 3.7.1.3 Procedure

In this follow on study, participants were asked to imagine that they were in a gift shop about to buy a surprise gift for a friend. While they were in the shop, their phone beeped. This was a message from their friend, the intended recipient of the gift, asking where they were. Two possible response options were presented to participants to disclose. These were:

i. Disclosing an completely untrue location, and
ii. Disclosing an intentionally blurred location.

In each scenario, participants were asked to assume that there was a **high possibility or very little possibility** that their friend or intended recipient will discover that they had not been entirely honest in disclosing their location. The aim of such a scenario was to find out if deception detection was an issue of concern to participants or ethics played a significant role in the level of discomfort. Since the participants and mode of administration of this brief study were the same as the previous study (using The Open University's *ELSA* system), refer to Sections 3.1 – 3.4 for further details of this study.

### *3.7.2 Findings and Discussions*

Data was extracted using *SPSS*, a statistical tool used in data analysis. Details of the processed data are found in *Appendix C*. In this section, we present sanitized data for the purpose of articulating the key observations of this sub-study.

#### 3.7.2.1 Deception Detection and Level of Discomfort

These scenarios used a Likert scale of 1 to 5, where ***1*** represents the situation in which participants have the least discomfort with the use of deception to protect location privacy, whereas a score of ***5*** represents a *very high level of discomfort.* Results extracted from the data presented Table 3.9 (see also Appendix C) and illustrated in Figure 3.7-1 below show that for a scenario in which there is a high possibility of deception discovery, there is a high level of discomfort using

the technique of deception to protect their location privacy. A Chi-square test confirmed this to be significant ($X^2 = 16.650$ (df=4), $P<0.05$). Refer to Appendix C.

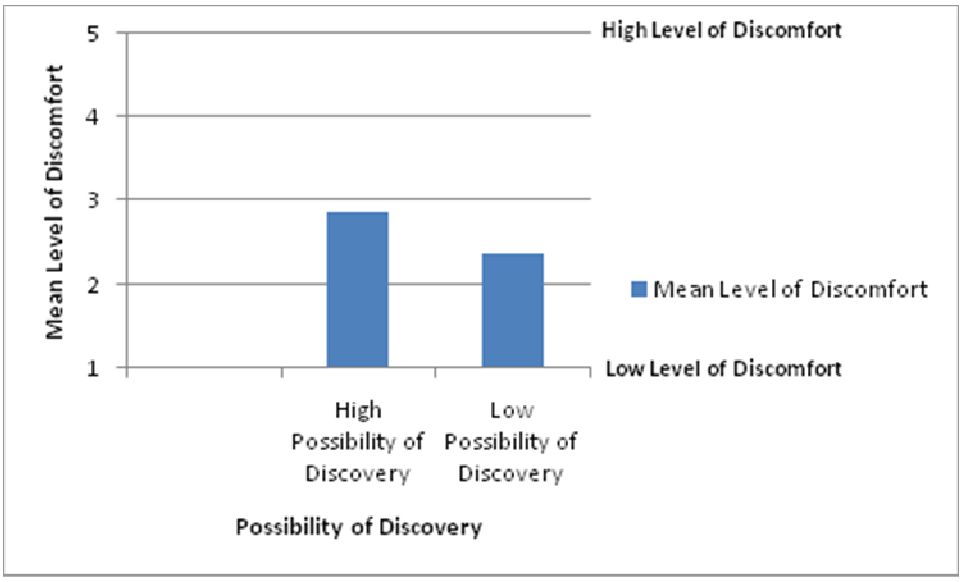


**Figure 3.7-1: Level of Discomfort Vs. Possibility of Deception Discovery**

**Table 3.8: Level of Discomfort for Different Possibilities of Deception Discovery**

| Possibility of Discovery | Mean Level of Discomfort | Standard Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| High Possibility of Discovery | 2.856 | 0.085 | 2.689 | 3.024 |
| Low Possibility of Discovery | 2.381 | 0.091 | 2.202 | 2.559 |

### 3.7.2.2 Effect of Location Privacy Protection Technique on the Level of Discomfort

Restricting the techniques used to protect location privacy to explicit disclosure of an untrue location and intentionally blurring the location to the recipient, Figure 3.7-2 (and for that matter Table 3.10) shows that there was much lower level of discomfort in the use of blurring (2.321) than outright deception (a score of 2.916) at 95% confidence interval. A Chi-square test confirmed this to be significant ($X^2 = 23.219$ (df=4), $P<0.05$). Refer to Appendix C.

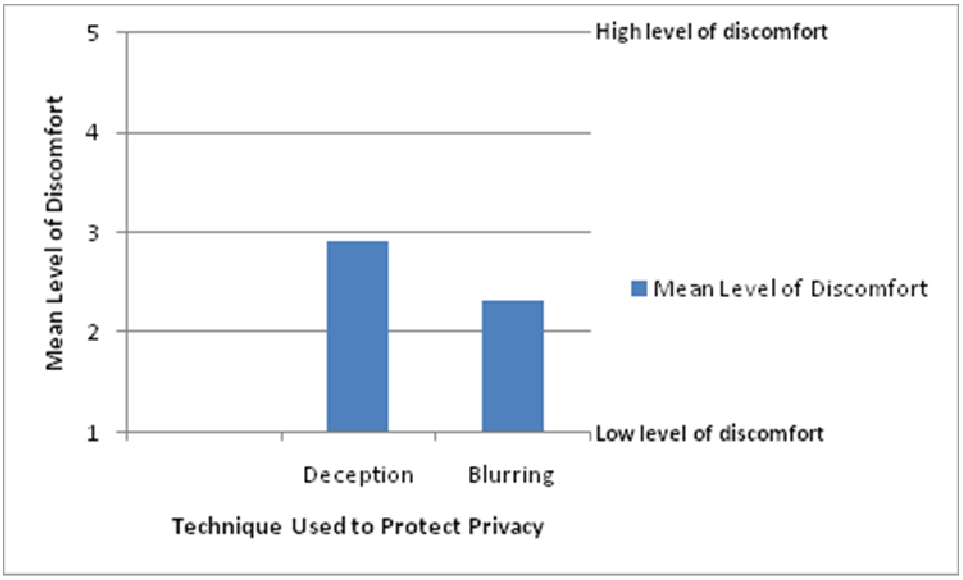


**Figure 3.7-2: Level of Discomfort Vs. Location Privacy Protection Technique**

**Table 3.9: Mean Level of Discomfort for Various Techniques of Location Privacy Protection**

| Technique Used to Protect Location Privacy | Mean Level of Discomfort | Standard Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| Deception | 2.916 | 0.086 | 2.748 | 3.085 |
| Blurring | 2.321 | 0.09 | 2.144 | 2.498 |

### 3.7.2.3 The Role of Ethics in the Use of Deception

In this part of the study, a score of ***1*** indicates that the scenario is perceived by the participant as very much an ethics issue, whereas a score of ***5*** is perceived not to be an ethics issue. The average mean for this scenario was 3.104 and a standard error of 0.089 at 95% confidence interval. A low possibility of deception detection scenario was perceived to be less of an ethics problem (i.e. a score of 3.238, above the avearge mean level of ethics concern) than a scenario with a high possibility of detection (2.971, i.e. below the average mean level of ethics concern) during an explicit deception disclosure. However, using blurring as a technique, there was less ethics concern for both scenarios of low and high possibility of detection. This is further illustrated in Figure 3.7-3 below. A Chi-square test confirmed this to be significant ($X^2 = 35.342$ (df=4), $P<0.05$). Refer to Appendix C. However, a Chi-square test between the level of ethics concern and the possibilities of deception detection showed that the difference in level of ethics concern is not significant.

**Table 3.10: Mean Level of Ethics Concern for High and Low Possibilities of Deception Detection**

| Mean Level of Ethics Concern | | |
|---|---|---|
| Scenario | Deception | Blurring |
| High Possibility of Detection | 2.971 | 3.875 |
| Low Possibility of Detection | 3.238 | 3.872 |

Average Mean = 3.104; Standard Error = 0.089

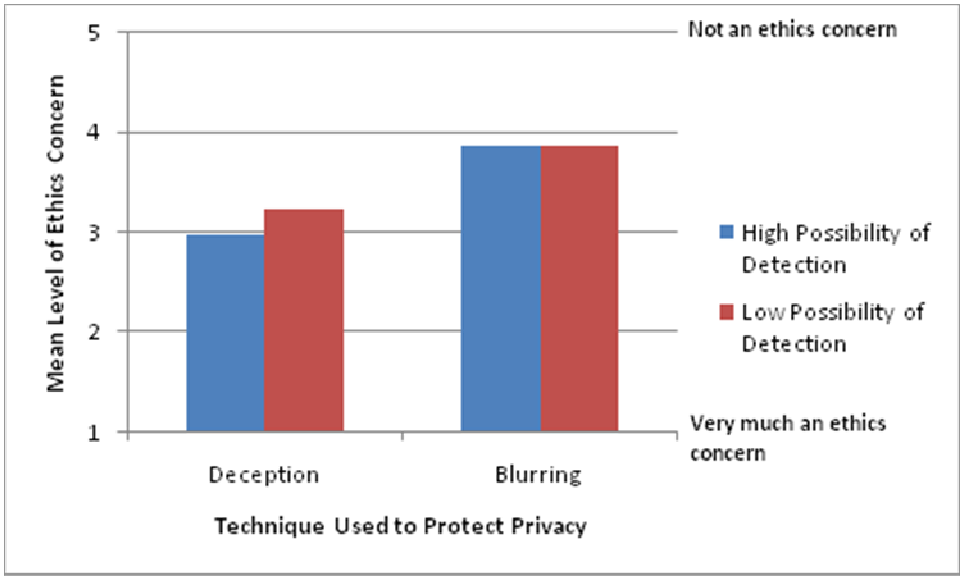


**Figure 3.7-3: Ethics Concern Vs. Techniques and Possibility of Discovery**

### 3.7.2.4 Summary

Evidence from the above discussion shows that:

a. When the possibility of discovery of deception in a location disclosure is high, the level of discomfort in engaging in deception is also high, compared to a lower possibility of discovery which has a lower level of discomfort.

b. The level of discomfort in employing blurring as a technique was lower than that with outright deception.

c. The data suggests a lower ethics concern with intentional blurring than outright deception.

The above observations provide a background for the design of deception-based techniques to protect location privacy, in particular, with the intent of reducing the level of discomfort.

## 3.8 The Role of Strategic Deception in Location Disclosure

**Table 3.11: Disclosure Factors Influencing Strategic Deception**

| Disclosure Factor | Frequency | Percentage (%) |
|---|---|---|
| Location of Requestor | 38 | 11.3 |
| Reason for Request | 264 | 78.8 |
| Don't Want to Know | 14 | 4.2 |
| Other | 19 | 5.7 |

Strategic deception is the type of deception which takes advantage of prior knowledge of the victim's context to employ a more plausible and difficult to detect type of deception (Christian & Young, 2004). Knowing the requestor's context (location in this case) makes it easier for the choice of a difficult to detect location, which makes sense at the same time. However, a key challenge in designing strategic deception for social mobile location systems is how the knowledge of context is presented in order to prevent the victim from knowing (the discloser in this case).

To investigate the usefulness of this kind of deception participants were asked what information about the requestor they will want to know before disclosing their location (assuming it was possible to know such information on their mobile phones). This was conducted with further assumptions that:

- the discloser knew the identity of the requestor
- the requestor was a member of the discloser's social network

These assumptions were made because previous research shows that knowledge of the requestor's identity is a significant factor in determining how location is disclosed (Lederer, 2003). Hence, I set out to investigate if the requestor's location and the reason for a location request formed an integral part of the disclosure process.

78.8% of the 335 participants who attempted this section stated that they would like to have prior knowledge of the reason for a location request before making a disclosure, whilst 11.3% would be interested in the approximate location of the requestor. However, 4.2% did not want to know anything prior to making a disclosure and 5.2% would want to know disclosure factors other than the reason for a request and location of requestor.

Therefore based on the above, we say that if strategic deception is described as having prior knowledge of the context of the requestor, then the factors that are likely to affect it are *reason for a request and the approximate location of the requestor.*
In this case, study 1 revealed that 89% of people will find it useful to know the approximate location of requestor and the reason for a request prior to disclosing their location.

## 3.9 The principle of strategic deception (PSD) in plausible location disclosure

A key feature of the concept of *strategic deception* is the knowledge of the victim or in this case the requestor (recipient of the disclosed location). This is about knowledge of who is making the request (enquirer), knowledge of the particular situation during the time of request, knowledge of the location of the requestor, and knowledge of the *face* of the requestor (Lederer et al., 2003). Lederer describes the metaphor of *situational faces* in which for every situation, a person wears a face as an abstraction of a set of privacy preferences. Whenever a person changes their privacy preferences, they are deemed to be changing faces, according to Lederer. A lot of empirical work has been carried out and the dependence of location disclosure on the *enquirer*, the *situation* and *face* has already been established (Lederer et al., 2003). Hence, basing our assumption on this fact, the knowledge of the requestor's location becomes the only interesting phenomenon to investigate in strategic deception. Therefore we define the Principle of Strategic Deception (PSD) as:

*In social mobile computing, if **A** requests to know the location of **B**, in order to disclose an ethically prudent, appropriate, and plausible location to **A**, **B** should have a fair idea of where **A** is.*

Irrespective of whether the disclosed location is false or not, the above statement will hold.
The advantages associated with the use of strategic deception include:

1. Avoiding the disclosure of too much information, e.g. a request comes from someone in another continent. It may not be useful disclosing a fine-grained location such as "I'm at Tesco, Kingston". Rather, it may be more useful saying, "Milton Keynes, UK" or just "UK".
2. Avoiding ambiguity in location disclosure. Knowing an approximate location and reason for a location request will help the disclosing entity (can either be the mobile device or person disclosing location) to avoid sending ambiguous disclosures to the requestor. Examples include disclosing a location as just "at the shop" or disclosing a more specific location such as "at ASDA, MK" depending on who is making the request, where the requestor is, and the reason for request.
3. Plausible deniability. To be able to disclose a false location that is plausible enough, it will be useful for the disclosing entity to know an approximation of the location of the requestor and the reason for request.

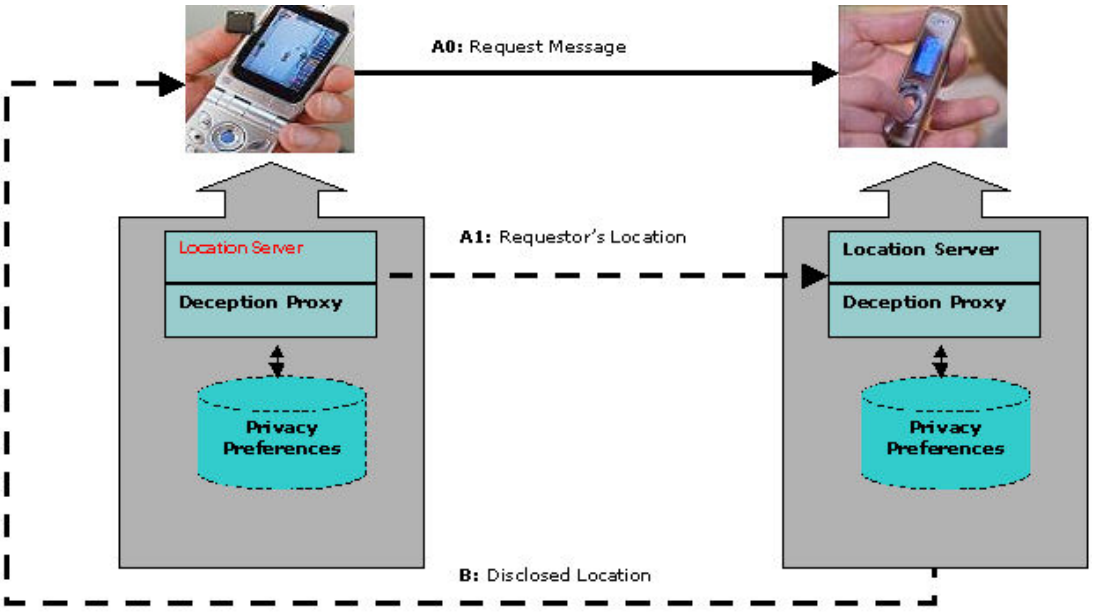


**Figure 3.9-1: Usage Scenario Describing How a Request and Disclosure are Made Between Two Mobile Client Users.**

Figure 3.9-1 above illustrates how the PSD is implemented within the mobile phone platform. First, a request A0 is sent with the requestor's location in a different message using a different port number such that the recipient of the request does not see it him/herself. A1 is only sent between the discloser engines of the requestor and discloser. This message does not get into the native messaging inbox of the user's phone because it is a control message or signal of some sort. As the concern of our design is not to inhibit established social practices, the control message should not be seen to be interfering with the request/disclosure interaction.

Figure 3.9-2 below describes the flow of execution of the various components of the architecture of the deception-based privacy control (DPC) model in a PSD setting.

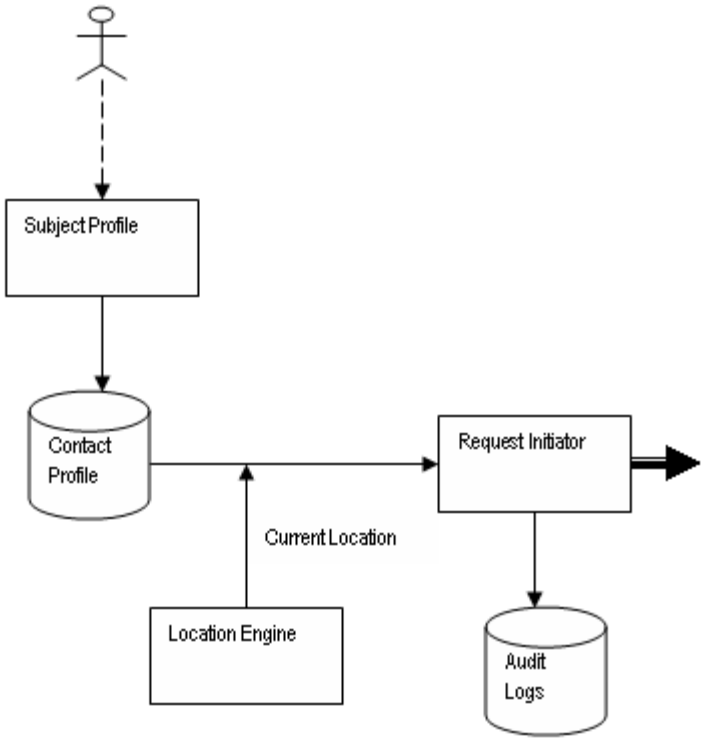


**Figure 3.9-2: Process Flow of the PSD Involving Components of the DPC Model's Architecture**

## 3.10 Conclusions

In this study, three scenarios were presented to study participants with response options on a scale of 1 to 5. Each scenario was further divided into two sub-scenarios, namely, how likely participants will be to engage in deception when a location request comes from one of 7 members of a typical social network (spouse/partner; boss; parent; child; colleague; friend; other family). **1** on the scale meant either "very likely" or "low level of discomfort" whilst **5** meant "not at all likely" or " high level of discomfort".

The analysis described in this chapter provides some empirical insight as to the extent to which deception can protect location privacy. This section sums up an evaluation of the findings of the study relative to the key goal indicators set out in Section 3.3, namely:

- The likelihood of the use of deception across the three scenarios.
- The level of discomfort expressed after engaging in deception across the three scenarios.
- The percentage of study participants who will engage in deception or forms of it to protect their privacy

In addition, the role of strategic deception in designing for deception is also summarised in this section.

#### 3.10.1.1 General Location Disclosure

An evaluation of the findings of the above study reveals that:

a. People will disclose their exact location to location requests coming from very close members of their social network, namely, spouse/partner, children, and parents. For location requests coming from all the other members of the discloser's social network (i.e. friends, workplace colleagues, workplace bosses, other members of the family, and strangers) the other disclosure options are more popular than an exact location disclosure.
b. Explicitly false location disclosure is not a popular technique of protecting location privacy as evidenced in the analysis. However, there is still a significantly small percentage of people that will deliberately disclose a completely false location to strangers.
c. People will, if at all, consider obfuscating their location information during disclosures, then the deliberate withholding of some location information or intentionally blurring location accuracy is a significant technique in protecting location privacy, according to the above analysis. Blurring is a popular technique for requests coming from closed family members as well as strangers.
d. Ignoring location requests is hugely popular with requests coming from strangers. Therefore, as expected, people will most likely ignore requests coming from those they do not know for various reasons, such as the fear of being stalked, harmed, or even being bombarded by location-based unsolicited messages by complete strangers, among others.
e. The analysis revealed that there are not many disclosure strategies apart from those mentioned in the study. A popular strategy that participants mentioned was to switch off their phones if they did not want to be bothered. Though switching off the phone is not always the best option, this can be useful in some circumstances.

#### 3.10.1.2 Strategic Deception

Empirically, the analysis shows that factors influencing strategic deception are *the reason for a location request* and *the location of requestor* at the time of request. This is based on the assumption that the identity and relationship of requestor are known by the discloser, since location information helps determine people's activities (Liao et al, 2005). Therefore, the reason for a location request can be inferred from the requestor's location and therefore their activities. Hence, location is a crucial strategic deception factor.

3.10.1.3 Patterns Identified in three Scenarios

a. When disclosing a false location with a good intent during a location request, people are less likely to do so to their parents or children than they would to their friends, spouses/partners, other family members, workplace bosses, workplace colleagues or strangers.
b. People experience a higher level of discomfort with disclosing a false location for good purposes to their children, parents or spouses/partners than they would for other members of their social network.
c. People are more likely to make a false location disclosure to enhance social harmony when they are confronted with location requests coming from their workplace bosses, colleagues, and friends than they would with other members of their social network. However, they will be more uneasy with making such disclosures to very close family members such as spouses/partners, parents, children, and other family members.
d. In scenarios other than disclosing a false location with a good intent or to enhance social harmony, people will be more likely to make false disclosures to workplace bosses or colleagues than the rest of their social network.

In conclusion, the high likelihood of engaging in the use of deception across the three scenarios for requests coming workplace colleagues, bosses, friends, and other family members, makes this technique a useful one to control location privacy. However, the high level of discomfort for the use of false disclosures to spouses/partners, parents, and children make its use problematic in location privacy protection. An attempt has been made to unearth the reasons for this high level of discomfort. Notable among these are:

i. whether explicit deception is used or intentional blurring
ii. a higher possibility of deception detection suggests a higher level of discomfort, and vice versa.
iii. Ethics does not play a significant role in raising the level of discomfort. From the evidence gathered, ethics only plays a key role when the technique used has a high possibility of the disclosure being detected by the intended recipient.

The patterns identified above inform the design of a deception-based privacy control (DPC) model in Chapter 4, followed by its implementation as the Mobile Client application, which is based on a request/disclosure dialogue between two or more people belonging to the same social network. Then Chapters 5 and 6 describe the user and expert evaluation of Mobile Client prototype, developed on design guidelines based on the DPC model.

# *Chapter 4. Deception-Based Location Privacy Control Model*

## 4.1 Introduction

In Chapter 2 I described the absence of established social practices as a challenge in the design of various privacy protecting mechanisms in the mobile computing environment. Chapter 3 provided evidence that deception can be a social practice in certain circumstances. In this chapter, I present a theoretical model based on deception using a classical military deception strategy. The model (called the Deception-based Privacy Control (DPC) model) is based on two key strategies of deception implementation, namely, *a-type* (ambiguity-type) and *m-type* (mis-direction-type) deception strategies, abstracted from Daniel & Herbig (1982).

The model is implemented in the Mobile Client application as a proof of concept. It must be emphasised that the proposed deception-based model is not a perfect or absolute privacy protection solution, but instead, complements the efforts of other researchers such as Lederer, (2003), Smith (2005), Langheinrich (2002). The model is meant for protecting the privacy of individuals of close social ties (especially within the same social network) who choose to have flexibility in the control of the disclosure of their location information, where necessary. As such I chose to concentrate on asynchronous location request and disclosure settings, typically in the form of a text messaging service for request/disclosure interactions (examples of such services are the MobileLocate, Friend Finder, ChildLocate, etc). The model is not meant for sensor-based environments where control over location cannot easily be achieved with existing mobile user interfaces.

## 4.2 General Overview and Requirements

In order to provide some understanding of the DPC model we discuss in this section the requirements for the design of deception with the help of a working scenario.

*4.2.1 Working scenario:*

Wilma is Fred's wife. To take advantage of the modern location-based service that their city service provider (Bedrock Telecoms) provides, they both have Mobile Client software installed on

their mobile phones, to be able to manually or automatically locate each other, their daughter Pebbles, and friends Barney and Betty, who also have become fans of Bedrock Telecoms' latest service. Whilst in a gift shop to buy Wilma a surprise birthday present, Fred's phone beeps. It's Wilma who wants to know where Fred is. Disclosing his true or actual location means that Wilma will find out to some extent what Fred is up to. One option is to ignore the location request. However, knowing what implications Wilma may draw from such behaviour, Fred would rather prefer disclosing a plausibly untrue location while maintaining the real essence of the surprise present, which at this time, is paramount to him.

With Mobile Client, Fred has several options to disclose a plausible location that is different from his actual location, while making it difficult for Wilma to detect that the disclosure is false. In the DPC model, Fred is able to make a:

- disclosure of a **completely false** location
- disclosure of a **false location plus an activity or context**
- disclosure of an **ambiguous location** by blurring or presenting a coarse-grained location
- disclosure of an **ambiguous multi-name** location, where possible.

### *4.2.2 Requirements for the Implementation of Deception*

For any of these disclosures to be effective and not be detected easily,

- Fred should be able to free his conscience that the false location disclosure is for a good or ethical purpose.
- Fred should be convinced that Wilma has little or no chance of detecting that the location disclosure is false.
- Fred should have a fair idea of Wilma's current location, in order not to disclose a location that could potentially make Wilma disbelieve him.
- Fred should be able to know whether such a disclosure is **appropriate** for Wilma under such a circumstance or not.

In order to achieve the above requirements, we propose a theoretical model based on the assumption that deception is an established social practice in general location disclosure, and a five-layer disclosure approach.

## 4.3 Deception-based Privacy Control Model

The proposed DPC model encapsulates the requirements outlined in Section 4.2 and is based on two key approaches, namely:

i. A five-layer disclosure approach

ii. Ambiguity-type and Misdirection-type disclosure strategies

The five-layer disclosure approach is based on the location sensing capability of the Global System for Mobile Communications (GSM) technology. Section 4.3.1 therefore provides some understanding of how a mobile phone user's location is typically determined using cell IDs.

### *4.3.1 Location Sensing Using GSM Global Cell IDs and GPS Coordinates*

The DPC model is based on a simple combination of global cell IDs and GPS coordinates for location determination. Within a specific spatial constraint, the location of a person or object is determined by their proximity to a known point of reference which can further be determined by wireless or physical contact (Roussos, 2002). In GSM mobile networks, such a reference point is usually called the base station. The diagram in Figure 4.3-1 below shows mobile phone base stations (represented by Δ) belonging to different networks in a section of Milton Keynes, a town in the south east of the United Kingdom. Base stations belonging to a particular network provider are connected in a cellular fashion in the form of a cluster as shown in Figure 4.3-2 below. Each mobile phone user must be connected to a base station in a cell to be able to make communications. Users are often located by the cell they are connected to.

Two types of location representation exist. These are physical and semantic locations. Physical locations are described by the latitudes, longitudes, and sometimes the physical elevation, e.g. 52' 11"N by 0.52' 23"E at 6m elevation. Semantic locations on the other hand describe the human-readable representation or description of a place either by place semantic (e.g. M Block of the Open University, Walton Hall) or geographic or physical semantic (e.g. a postcode MK7 6AA) (Roussos, 2002). In the five-layer disclosure approach, locations are represented by place semantics rather than physical semantics.

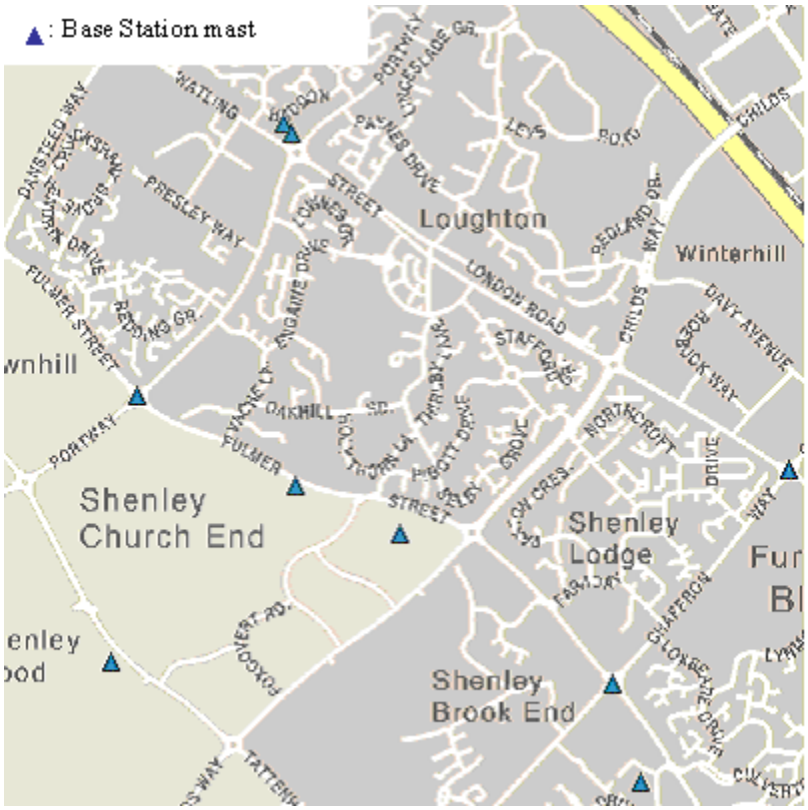


**Figure 4.3-1 A Map Showing GSM Station Mast Positions in Parts of Milton Keynes, UK**

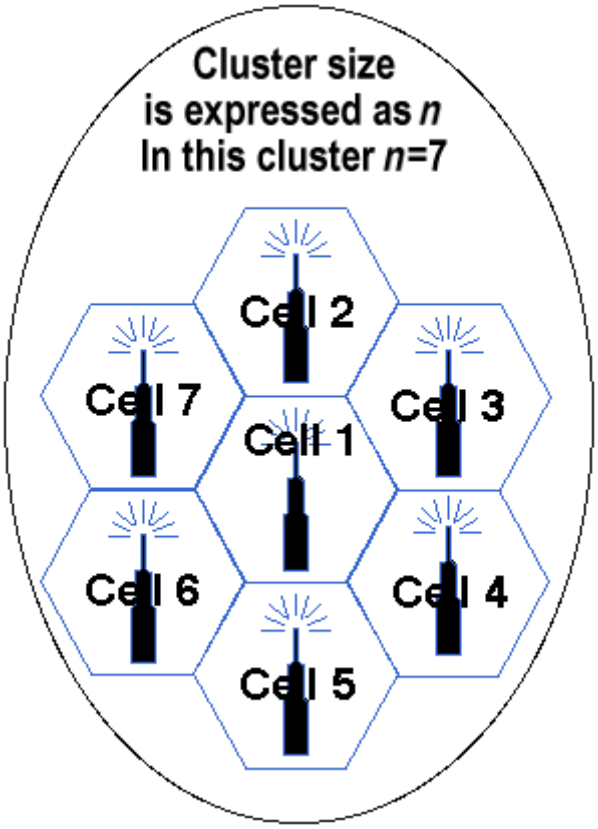


**Figure 4.3-2: Structure of a Cell in Mobile Network Systems**

Having equipped ourselves with the rudiments of location sensing using the GSM technology, we now move on to describe the five-layer disclosure approach and how it relates to the DPC model.

## 4.4 5-layer Disclosure Approach

The mechanism for the disclosure of location is based on a modified version of the work of Smith et al (2005) and that of Laasonen *et al* (2004*)*. In making a disclosure, the design requirements for deception outlined in Section 4.2.2 above are applied to a disclosure matrix (described in Table 4.1 below). In this way, the disclosed location has a greater chance of being ethically prudent, plausible, strategic, and appropriate for most contexts.

In this approach, disclosure is based on a five-layer method corresponding to the granularity of location detail to be presented to the requestor. This is based on our experience in the use of a prototype we built on the Placelab tool (Intel, 2004) and on the limitations of existing GSM infrastructure. "*Place Lab is software providing low-cost, easy-to-use device positioning for location-enhanced computing applications. Place Lab tries to provide positioning which works worldwide, both indoors and out (unlike GPS which only works well outside). Place Lab clients can determine their location privately without constant interaction with a central service (unlike badge tracking or mobile phone location services where the service owns your location information)" (Intel, 2004).* The 5-layer approach uses the combination of global cell ID and the GPS coordinates in the following format:

MCC:MNC:LAC:CI:α……..1

These correspond to:

a. Mobile Country Code (MCC)
b. Mobile Network Code (MNC)
c. Location Area Code (LAC)
d. Cell Identifier (CI)
e. **α** is a description of the geographical coordinates of the user (and not the base station).

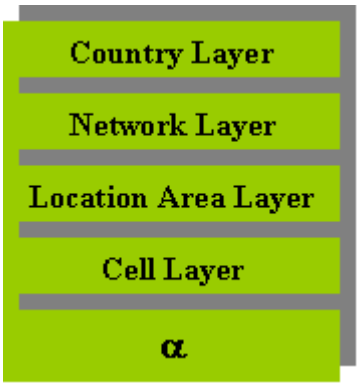


**Figure 4.4-1: 5-Layer Disclosure Model Based on Cell ID Parameter (Signature) Comparison**

The highest layer for location comparison and subsequent disclosure is the country layer (refer to Figure 4.4-1 above). A key element of the country layer is the Mobile Country Code (MCC). This is a numeric string of size 3. If the requestor comes from a different country (as captured in the cell signature), then a more plausible and appropriate location to disclose will be a coarse-grained type, e.g. a request coming from Seattle, US to a discloser in the UK could appropriately be addressed simply by saying "I'm in Bath, UK", and this perfectly makes sense. However, such a reply may not have the desired effect if it were meant to a request from the same country. This is where the use of the network and location area layers comes in.

Since more than one GSM service provider exist in many countries, the network layer enables a location disclosure engine to determine the service providers of both the requestor and discloser. The Mobile Network Code (MNC), a two numeric string, is used to identify the *network layer*.

The *location area layer* described by the Location Area Code (LAC), an integer between 0 and 65535 inclusive, describes the code allocated to a particular town or city for a specific network provider in a specific country. The same town or city can have different LACs, one for each network operator.

A finer-grained area, the *cell layer*, is that covered by the base station itself, called the cell and often described by the Cell Identifier (CI), which is an integer between 0 and 65535 inclusive. Based on the signal strength of the base station with respect to a mobile user and the fixed geographical coordinates of the base station, a mobile network subscriber's position can be determined from a few metres to 30km. This is where the next layer, the ***α*** *layer*, becomes significant.

The **α** layer is a description of the geographical coordinates of the user (and not the base station). GPS coordinates are collected over a cell layer, and then the whole location area into a database. Such databases are available for download from wiggle.net and maps.google.com. However, additional place semantics may have to be defined where necessary, since some of those defined in these databases may not accurately describe the same semantics for every person. It is expected that as more phones get equipped with GPS capability, semantic locations can easily and more accurately be described.

Table 4.1 below describes a matrix for location disclosure based on the relative positions of the requestor and discloser. These relative positions represent different scenarios and which layer-based signature to disclose for true and plausible disclosures; ambiguity-type disclosures; and misdirection-type disclosures. For example, when a request comes from say, Alice (of location

coordinates MCC:MNC:LAC:α) to Bob (of location coordinates MCC:MNC*:LAC*:α*), in the five-layer approach, their signatures are first compared before any disclosure is sent to Alice. MCC is the same for both signatures. However, MNC:LAC:α are different. Hence, scenario #2 will be chosen for disclosure. The location disclosure process is further illustrated in a flow diagram in Figure 4.4-2 below. Actual disclosure is done based on the set preference for Alice on Bob's phone. For a simple flow process based on preferences, refer to Figure 4.4-3 below. If Bob sets Alice's request to disclose the true location, then a place semantic based on the signature **LAC:CI:α** is presented to Alice as the disclosed location. For an ambiguity-type disclosure, a place semantic based on either **LAC** or **LAC:CI:α** is disclosed. Better still, for a misdirection-type location disclosure, one of four possibilities (i.e. LAC, LAC*, LAC:CI, LAC*:CI*) will be disclosed together with a context or activity, thus, stressing how truthful the disclosure is.

To further provide some understanding in the use of the DPC model, the following describes a usage scenario based on Daniel & Herbig's (1982) misdirection (m-type) and ambiguity (a-type).

## *4.4.1 Usage Scenario*

In this section, we present two scenarios to illustrate how the DPC model is used to make requests and disclosures.

#### 4.4.1.1 Ambiguity-type Disclosure

Ambiguity-type disclosures are divided into two types namely:

i. Blurring of the actual location or presenting a coarse-grained location.
ii. Disclosing a multi-name multi-location

Referring to the scenario in Section 4.2.1, Fred is able to prevent Wilma from knowing his actual location by employing either of the two ambiguity-type disclosures. Since they both live in Bedrock and subscribe to Bedrock Telecoms, their locations will always have the same MCC, MNC, and LAC. However, their CI and α will change as they move about in Bedrock. Hence, in choosing to disclose an ambiguous location to Wilma, a human-readable representation of the CI will achieve the same purpose of keeping the surprise while at the same time Fred becomes comfortable with having to present a less truthful or exact location to Wilma. This also satisfies the notion of importing established social practices into design. In real life situations, without the use of the Mobile Client, Fred will be able to say, "I'm at the City Centre" instead of "I'm at the Hallmark Gift Shop".

Fred is also able to disclose a multi-name multi-location on condition that such a location is ambiguous enough to prevent Wilma from knowing exactly what Fred is up to. The conditions for use of this option are as follows:

i. The location should not reveal the exact activity of the person. In other words, it should be difficult for Wilma to tell exactly what Fred is doing. For instance, "I'm in Asda", "I'm in Tesco", etc. In this case Wilma will not be able to tell exactly what Fred is doing in Asda or Tesco.
ii. The location should have the same name in two or more other locations within the same LAC. In this case Wilma will not easily be able to tell which Tesco or Asda Fred is in, using the disclosures in (i) above.

#### 4.4.1.2 Mis-direction type Disclosure

This type of disclosure is basically the addition of context information (usually an activity) to the actual location, false location, or an obfuscated form of the location (through blurring or otherwise). As described earlier in Chapter 2, the purpose of this is usually to improve the perceived truthfulness of the disclosed location. In this case, we are more interested in the use of context to enhance the perceived veracity of a false or obfuscated location.

In our working scenario, Fred can employ this strategy by appending an activity to his false disclosure, say, "I'm at Starbucks drinking my favourite Mocha and thinking of you". This is implemented using any false disclosure matrix output plus a human-readable context activity.

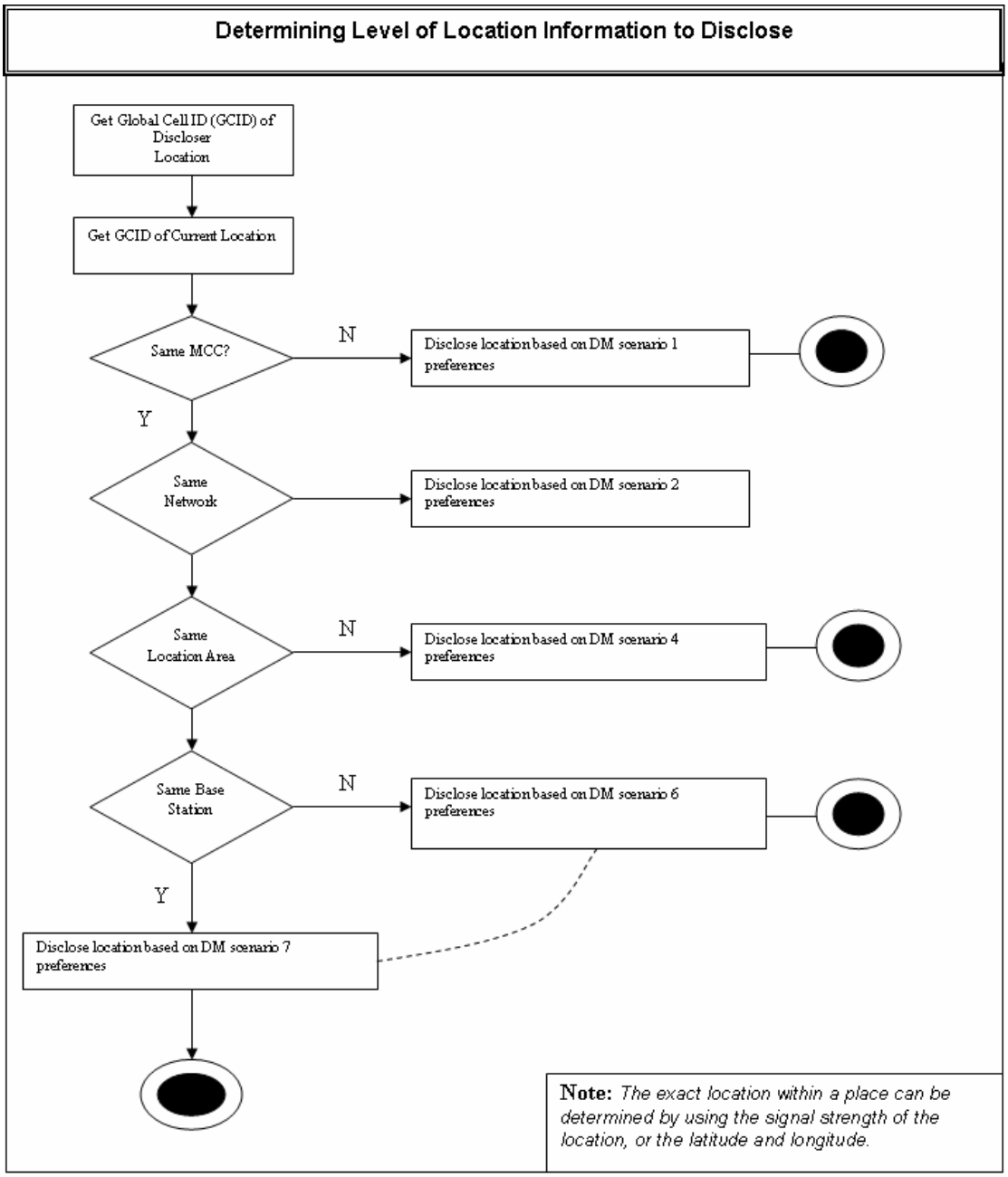


**Figure 4.4-2: Execution Flow of Location Disclosure Process.** This describes the flow process for disclosing a location using the Disclosure Matrix (DM) described in Table 4.1.

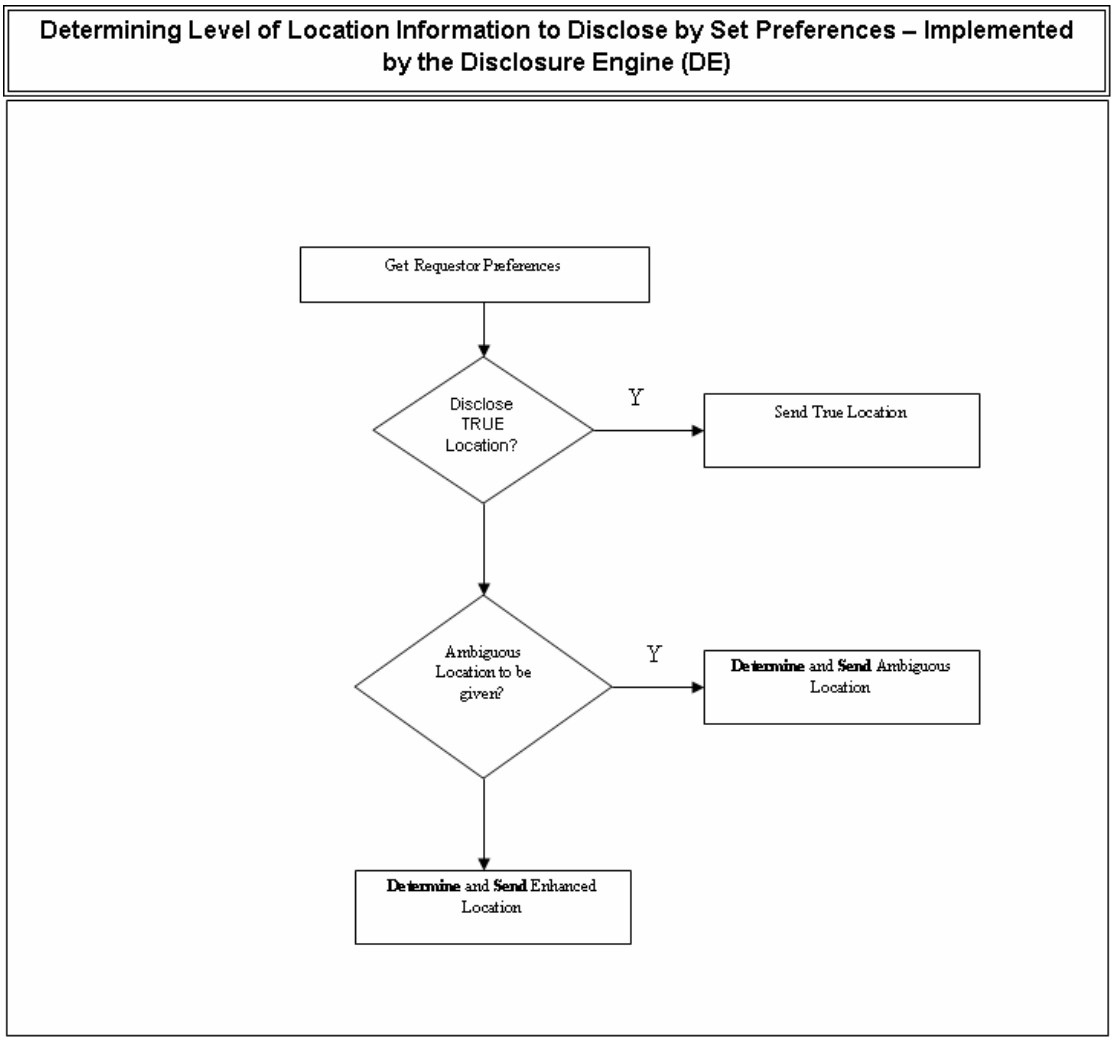


**Figure 4.4-3: Disclosure Flow Process by Preferences.** This outlines broadly the disclosure of a location, based on the set preferences for a particular request.

**Table 4.1: Disclosure Matrix (DM) Based on the 5-layer Disclosure Model**

| **Scenario no.** | **Requestor/discloser relative locations with respect to location signatures** | **True and Plausible Disclosure** - Semantic location based on: | **Ambiguity-type disclosure** (based on a coarse-grained human-readable location ) - Semantic location based on: | **Misdirection-type disclosure** - Semantic location based on: |
|---|---|---|---|---|
| 1 | Different MCCs | MCC:LAC:CI:α | i. MCC:LAC<br>ii. MCC | i. MCC:LAC + Activity/Context<br>ii. MCC + Activity/Context |
| 2 | Same MCC but different MNCs | LAC:CI: α | i. LAC:CI<br>ii. LAC | i. LAC:CI + Activity/Context<br>ii. LAC + Activity/Context<br>iii. LAC*:CI* + Activity/Context<br>iv. LAC* + Activity/Context |
| 3 | Same MCC and same MNC | LAC:CI: α | i. LAC:CI<br>ii. LAC | i. LAC:CI + Activity/Context<br>ii. LAC + Activity/Context<br>iii. LAC*:CI* + Activity/Context<br>iv. LAC* + Activity/Context |
| 4 | Same MCC, same MNC, but different LACs | LAC:CI: α | i. LAC:CI<br>ii. LAC | i. LAC:CI + Activity/Context<br>ii. LAC + Activity/Context<br>iii. LAC*:CI* + Activity/Context<br>iv. LAC* + Activity/Context |
| 5 | Same MCC, same MNC, and same LAC | CI: α | LAC | i. LAC + Activity/Context<br>ii. LAC* + Activity/Context |
| 6 | Same MCC, same MNC, same LAC, different CIs | CI: α | LAC | i. LAC + Activity/Context<br>ii. LAC* + Activity/Context |
| 7 | Same MCC, same MNC, same LAC, same CI | A | LAC | i. LAC + Activity/Context<br>ii. LAC* + Activity/Context |

(LAC)*: An obfuscated or completely different LAC other than the true or actual LAC-based location.

**Note**: There is only one instance of same MCC but different MNCs, because the same criteria will be used for such scenarios. Computationally, making location comparisons between different MNCs will require querying a larger location database (often involving another network provider) than is the case for same MNCs.

Table 4.2 below contains a list of places A, B, C, D, E, and F with their signatures.

**Table 4.2: Example of Location Signatures**

| Place | Signature | Latitude | Longitude | MCC | MNC | LAC | CI |
|---|---|---|---|---|---|---|---|
| A | 234:15:14307:23 | 56.0931 | -4.55462 | 234 | 15 | 14307 | 23 |
| B | 310:26:6183:111 | 47.0763 | -122.6952 | 310 | 26 | 6183 | 111 |
| C | 234:10:34788:4067 | 52.2191 | 0.0772 | 234 | 10 | 34788 | 4067 |
| D | 234:33:19713:183 | 52.2187 | -0.0128 | 234 | 33 | 19713 | 183 |
| E | 234:33:570:165 | 52.2185 | 0.1015 | 234 | 33 | 570 | 165 |
| F | 234:33:10749:165 | 52.2182 | 0.1021 | 234 | 33 | 10749 | 165 |

From the above table, the MCC of places A and B are different, signifying that they come from different countries or country layers according the model. However, A, C, D, E, and F all have the same MCCs but different MNCs, LACs, and CIs. D, E, and F have the same MNC or network layer, coming from the same mobile network operator, but belonging to different location areas and cells.

## 4.5 Implementing the DPC Model

The DPC model provides an additional layer of flexibility in location disclosure to support the established social practice of presenting an intentionally obfuscated or completely untrue location to protect privacy among other reasons. This gives users the ability to disclose their location in very similar ways as they would in real world social interactions. The features of the DPC model are described in Figure 4.5-1 below. The important feature of the DPC model is the implementation of the Disclosure Matrix (DM) based on the 5-layer disclosure model described in Section 4.4.

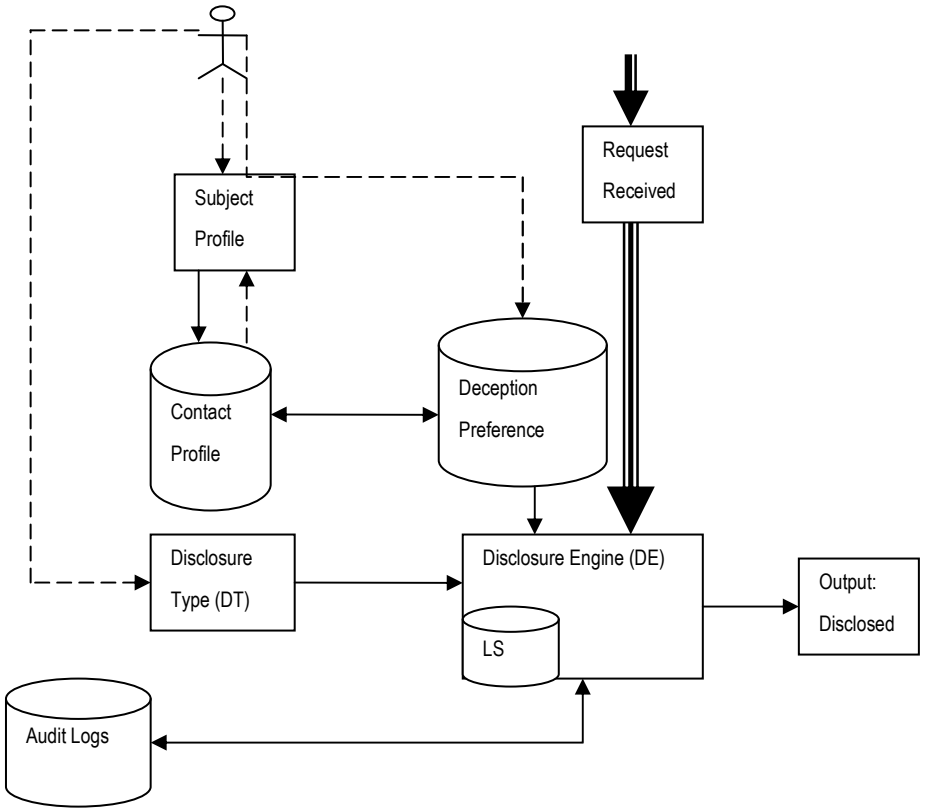


**Figure 4.5-1: Architectural Representation of the DPC Model**

## *4.5.1 Architecture Component description*

In this section, we describe the various components illustrated in the architectural representation of the DPC model.

**i. Subject profile**

The subject profile contains information that describes the owner of the phone. It holds the name of the bearer or owner of the phone, the phone number associated with the person and any personally identifiable information used to match requests or disclosures coming from the phone.

**ii. Contact profile**

The contact profile contains names and phone numbers of people the subject will be contacting. The equivalent of this is the phonebook and its contents within conventional mobile phones. The subject interacts directly with the contacts profile to make requests. Each contact profile has a set preference, stored in a deception preference profile.

**iii. Deception preference profile**

This profile contains the set of deception preferences that a subject chooses to set for each contact in the contact profile. Typical deception preferences include:

a. **Location blurring** – employing a coarse-grained location disclosure

b. **False location disclosure** – disclosing an explicitly untrue location
c. **False location disclosure and an activity** – a misdirection-type disclosure where location is disclosed with an activity or context to emphasise the truthfulness of the disclosed location.
d. **True location/True location and an activity** – to prevent others from having the notion that disclosure is all about false locations, the deception preference profile also contains a true location option.

iv. **Disclosure type** – Disclosures are either automatic or manual. Automatic disclosures rely on pre-set preferences for each contact and automatically compute a plausible location to a requestor. Manual disclosures present the subject with a screen to type in the desired location to be disclosed.
v. **Disclosure engine (DE) –** Location computations are done within the disclosure engine. The DE implements the computation algorithm based on the matrix in Table 4-1 above. The deception design principles mentioned in Chapter 3 as well as the DM, help present a plausible location that is ethically prudent, appropriate, and strategic.
vi. **Output –** The disclosure is displayed as output to be presented to the requestor.
vii. **Audit logs –** these are time- and date-stamped logs of requests made and disclosures received. This can be enabled or disabled where necessary.

### *4.5.2 The Mobile Phone Platform*

The choice of using the mobile phone platform for implementation is mainly for its increasing computation capability as well as the fact that it is carried by many people. Our reason for using the mobile phone is not very different from that by Smith et al (2005). However, the Mobile Client is built on Java 2 Micro-Edition (J2ME) with Mobile Information Device Profile version 2 (MIDP2) and Connected Limited Device Configuration (CLDC). Hence, it works in many different mobile brand platforms rather than on only Nokia Series 60 platforms as is implemented in Smith et al (2005). The disadvantages of debugging difficulty and limited storage still remain an issue, though the latter is increasingly becoming a less problematic issue.

In addition to it being a mobile social tool (Smith et al., 2005), the mobile phone satisfies many user interface design principles, and therefore presents the best option for implementing the DPC model.

### *4.5.3 Location Sensing*

Location sensing capability within the DPC model is twofold:

1. A GSM-based location signature consisting of the Mobile Country Code (MCC), the Mobile Network Code (MNC), Location Area Code (LAC), and the Cell ID (CI).
2. Physical coordinates made up of the latitude and longitude and represented as α.

Currently, there are several databases which contain locations with GSM location signatures as well as their physical GPS coordinates (e.g. placelab.org, wiggle.net, googlemaps etc). Until mobile phones are shipped with GPS functionality, locations of interest can be downloaded from any of these databases for manipulation during disclosure.
Like the Placelab project (Intel, 2004) the Mobile Client comes with a location store which is a database of places of interest with their location signatures. Determination of the location which is based on the associated tower the mobile phone is connected to, does not rely on any additional hardware or device. Location accuracy is improved with the introduction of α (physical GPS coordinates) to the GSM signature, to a few metres.

### *4.5.4 Coding environment*

Mobile Client has been built to facilitate the evaluation of the strategies outlined in the DPC model. It does not implement automatic use of the strategies as it is usually better first implementing such strategies manually before attempting automatic functionalities (Iachello, 2005). The development is in J2ME and J2ME Wireless Toolkit for the test environment. Since coding is beyond the scope of this research, details of the codes used are too bulky to be presented in the appendix.

## 4.6 Functional Testing of the DPC Model

Functional testing is basically the testing of a piece of software based on its functional requirements. This type of testing does not include code walkthroughs or specific details of the piece of software. It involves testing the key functionalities of the test target.
Functional testing of the Mobile Client key functionalities was conducted using the J2ME Wireless Toolkit. The initial scope of this test was limited to four key areas, namely:

i. **Requesting a location**
ii. **Preference setting (automatic or manual preference setting)**
iii. **Default port testing (native messaging)**
iv. **Disclosing a location**

However, the Wireless Toolkit could not be used to test disclosures as the test environment needed to be connected to a live network operator. Therefore only (i) and (ii) were tested successfully using the J2ME Wireless Toolkit.

I experimented with several versions of the interface using pilot subjects (postgraduate computing students) and iterated on the design until the pilot subjects were able to complete the tasks, then I began the evaluation. Figure 4.6-1 below shows a screen shot of making a request in the test environment. The contact profile of the test environment consists of one contact, "Armstrong", and the menu is made up of three options, *Request*, *Set Preferences* (for the selected contact), and *Delete*.


**Figure 4.6-1: Screen Shot From the Test Environment on J2ME Wireless Toolkit**

### *4.6.1 Limitations*

Like every implementation of a prototype, the limitations in the implementation of the DPC model are no exception. The following is a look at such limitations in the implementation of the DPC model in Mobile Client.

i. **Automated disclosure –** The purpose of this prototype is not to demonstrate whether or not automated disclosure is possible, but rather to evaluate a semi-automated form of the proposed strategies at work. Hong et al. (2004) recommend not to start with feature automation in social mobile location systems. Hence automatic disclosure was not implemented in the prototype although the option was displayed in the interface.

ii. **Preference logic activation –** The logic in the activation of deception preferences is not provided with the initial build of the Mobile Client prototype.

iii. **No inbuilt audit logs –** Inbuilt audit logs were not implemented as they did not contribute to the design decisions or interface behavior.

## 4.7 Summary

In this chapter**,** I proposed a deception-based privacy control model for protecting location disclosure. I have shown through a scenario how the requirements for good deception implementation are abstracted into guidelines for the design for deception in social mobile computing.

I have also proposed the use of a 5-layer disclosure model based on a modification of the global cell ID of GSM base station signatures and GPS coordinates. Deception design guidelines have been presented in the form of a disclosure matrix to aid in the design of an ethically prudent, appropriate, plausible and difficult to detect deception in social mobile computing.

The Mobile Client prototype, built as proof of concept of the DPC model was tested in the field by real users. In the next chapter, I describe details of the study and the role the model plays in preserving location privacy.

# *Chapter 5. Field-based User Evaluation of the Mobile Client Application*

## 5.1 Introduction

A field-based user study was conducted to determine the usefulness and effectiveness of the DPC model among users. Whereas Chapter 6 provides empirical evidence about the use of the mobile client with context-based scenarios in a laboratory environment, this chapter describes the use of the mobile client application in the field.

## 5.2 Objectives of the study

The aim of the user study was to test the acceptability of reasonable deception in the field. To what extent would people believe disclosures under different schemes? To what extent would members of a social group use personal knowledge in detecting deception? Would deception be detected or accepted in a genuine setting? Given the pragmatic constraints, the user study was intended as a 'proof of concept' rather than a full-scale validation.

Two pilot studies preceded the user study: the first was intended to test both the platform and the feedback system; the second was intended to familiarize the participants with the systems and to ensure that they were working in the actual study context.

## 5.3 Platform

The study was conducted on the Mobile Feedback platform {www.mobilefeedback.com}. A number of options were considered in order to effectively capture data that will be representative of a typical field-based user study, reducing as much bias as possible.

***Placelab***

A modified version of Intel Research's Placelab (www.placelab.org ) (Intel, 2004) was considered.

At the time of writing this thesis, Placelab was one of the best options (in the research community) to simulate real-time location requests and disclosures. However, multiple experiments with modified versions of Placelab showed that much greater programming effort is needed to tweak the application to suit our purpose. It was also unable to collect real-time data of participants' reactions to requests and/or disclosures in the field.

***M:Science***

A more light weight system of making requests and disclosures was therefore needed to undertake the user study within the timeframe at hand. The M:Science application (www.m-science.com) was considered as an option, having read their success stories in institutions such as Berkshire College and Salisbury College. The M:Science platform enables asynchronous text messaging and can be used to collect data in the field. However, setting up the SMS server in a trial version proved problematic.

***Mobile Feedback***

The Mobile Feedback system became an obvious choice since no configuration was required to undertake simple tasks with scenarios. The Mobile Feedback setup is a two-way asynchronous text messaging platform employing the capabilities of the internet and mobile telephony. The platform enables communication between a web user and one or more mobile phone users. The web user, usually called the system operator is able to interact with other users in a survey or study that requires pushing questionnaires to users in the field. It includes group management facilities, messages and questions input interface, processing of the results (the group answers to a question initiated by the operator), display of the distribution of answers, output analysis tools, distribution of results by Email and SMS, and storage facilities. Users can receive one-way SMS messages or SMS closed end or open questions. Answering these questions is a minimal task for the user, since he/she employs the "REPLY TO SENDER" function and is required to type in most cases a single digit number only (the number of the answer he/she choose)" (www.mobilefeedback.com).

Figure 5.3-1 below shows the architecture of the Mobile Feedback platform and the flow of information during a study. Questionnaires and scenarios are designed on the web-based platform and then pushed to mobile phone users via the internet and the Mobile Feedback infrastructure. The Mobile Feedback infrastructure consists of the Mobile Feedback Server and an SMS gateway. The SMS gateways relay these messages through mobile phone carriers or service providers to the targeted phones.

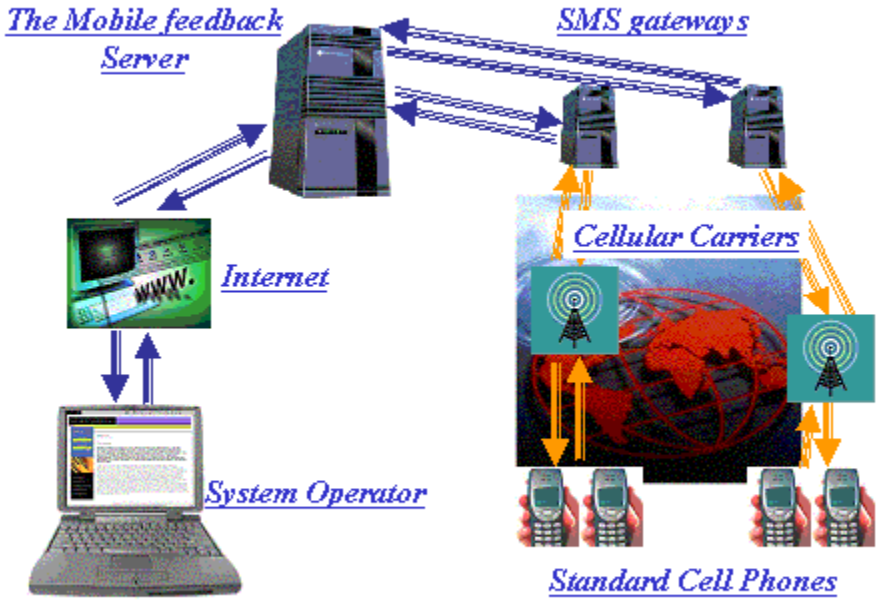


**Figure 5.3-1: Architecture of Mobile Feedback Operation – (www.mobilefeedback.com)**

Figure 5.3-2 shows a screen shot of the Mobile Feedback control interface with a number of sessions running, where each session is a feedback dialogue with an individual participant.

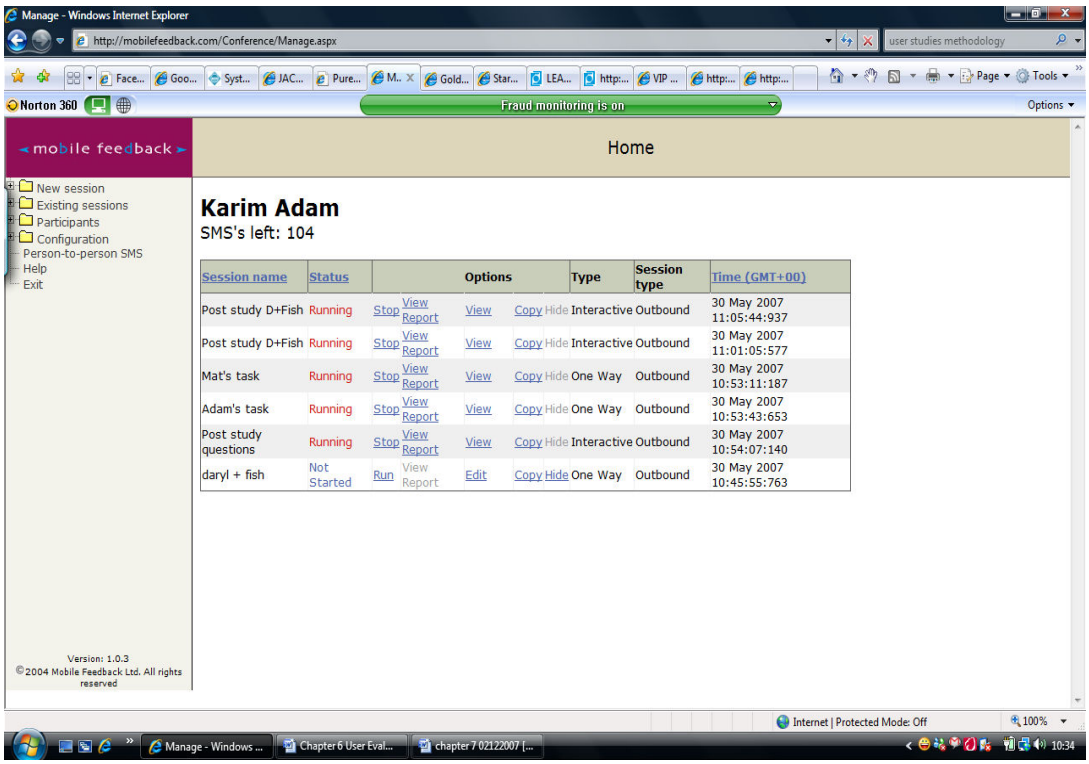


**Figure 5.3-2: Mobile Feedback Screen Shot of Log of Active Sessions**

## 5.4 Study Design

The study integrated three empirical methods (scenario-based task performance, questionnaires, and post-task interview) into the evaluation process. Combining methods allowed capture of data that would otherwise have been missed in using just a single method.

*Scenario-based task performance* [could participants use the disclosure strategies?]: Roles were assigned to participants, either 'requestor' or 'discloser' (so that only the 'disclosers' would know which mechanisms were employed in producing responses). Each day, participants were sent an alert as to what task they were to carry out that day. Each requestor was asked to make at least one request per weekday and a maximum of three requests per day at weekends. Each discloser was asked to use one particular form of disclosure for any requests during that day: true location, true location with activity, false location, false location with activity, or blurred location. Disclosers were given clear instructions to disclose plausible false locations, avoiding disclosures that would be easily detected as untrue by the requestors. Automated daily alerts were sent via the Mobile Feedback application.

*Questionnaires*: At the end of each day, participants were asked via Mobile Feedback how truthful they believed each disclosure they received on that day was.

*Post-task interview*: Each participant was interviewed after the study. Each was asked whether the responses they had made were those they had intended, with reference to the disclosure log. The aim of the interviews was probe the basis on which they assessed the truthfulness of disclosures and whether they used personal knowledge in doing so. Participants were also asked whether they considered that such an application would be useful in their daily life.

The study design and all documentation were reviewed and given ethics approval by the Open University Human Participants and Materials Committee.

## 5.5 Participants

The user study needed a pre-existing social network (so that participants could bring personal knowledge to bear in assessing the truthfulness of location claims) that was technology savvy (to reduce the intrusion of the technology on the focus of the study) and mobile (to either give rich enough location data, or make varied location data plausible). Therefore, groups of students from the local college and secondary school were identified.

*Pilot 1:* Two students, young adult males (ages between 17 and 18) who were friends, were recruited from the local further education college. Both were regular mobile phone users familiar with location-based technology.

*Pilot 2:* Four teenagers (ages between 17 and 18 and all male) were recruited from the local secondary school. These teenagers were friends and therefore belonged to the same social network, a pre-condition for a request/disclosure dialogue throughout this dissertation. All were regular mobile phone users familiar with location-based technology.

*User Study:* The same participants were used as for Pilot 2.

Although it would have been desirable to have conducted larger-scale studies with more social networks, pragmatic constraints such as the number of handsets available and the duration of the user study constrained the scale of the study. Under the circumstances, it is argued that one social network operating over a reasonable period was sufficient to demonstrate the concept and to reveal initial issues surrounding deception and location disclosure. No claims of generaliseability are made. The two pairs of requestors and disclosers were able to cover all disclosure strategies on more than one day each. Larger-scale, more detailed follow-up studies are left to future work.

## 5.6 Protocol

**1. Recruiting:** Participants were solicited at the local college and secondary school via university contacts with those institutions. A one-page outline description of the study was circulated via email and post (see Appendix E).

**2. Briefing meeting** (individual face-to-face meeting with each participant): Participants were introduced to the study, including the concepts of truth and deception in location information, and were invited to ask questions. Each was given an instruction sheet and each completed a consent form in order to 'opt in'. (see Appendix E).

Participants were equipped with a Nokia N70 phone with Mobile Client pre-installed. They used their own SIM cards. They were given mobile phone credit which exceeded the cost of the study. The use of the Mobile Client application was introduced, and participants were taken step-by-step through the necessary functions, such as making a request, a disclosure, setting disclosure preferences, and adding contacts. Disclosers were introduced to the disclosure strategies.

**3. Conduct:**

***Pilot 1.*** 1 week

The objectives of this pilot study were to test the various functions of the Mobile Client application (such as making a request, a disclosure, setting disclosure preferences, and adding contacts) and to test operation of the data collection platform. Participants were asked to make a variety of requests and to respond using any of the disclosure strategies, as they wished.

A total of 23 valid requests were processed over the one-week period. The numbers of requests per disclosure strategy are given in Table 5.1 All true locations were perceived as true. All other categories of disclosure were perceived as true or fairly true. Blurring was never used.

**Table 5.1: Disclosure Results from Pilot 1**

| Disclosure | number of instances | perception |
|---|---|---|
| true location | 9 | True |
| true location with activity | 7 | 3 true, 4 fairly true |
| false location | 1 | fairly true |
| false location with activity | 6 | fairly true |
| Blurring | 0 | |

The pilot study identified a number of minor technical issues with the Mobile Client application which were straightforward to address. The data collection operated as predicted. However, it became clear that a more structured request/disclose regime would be needed. Because both participants were fully briefed about the disclosure strategies, they reported that they were primed to question disclosures rather than trust them, even though they perceived all disclosures as true or fairly true.

***Pilot 2.*** 1 week

The objectives of this pilot study were to test the (now adjusted) functions of the Mobile Client application, to test the operation of the data collection platform, to test the new request/disclose regime, and to familiarize the user study participants with the phones, applications, and tasks. Roles were assigned to participants, either ‘requestor’ or ‘discloser’, in order to limit specific knowledge of the disclosure strategies to the ‘disclosers’. Instructions were sent by MobileFeedback in the form of a text message to each participant describing the tasks to perform on a daily basis.

A total of 35 valid requests were processed over the one-week period. All true locations were perceived to be true or fairly true. The numbers of requests per disclosure strategy are given in Table 5.2.

**Table 5.2: Disclosure Results from Pilot 2**

| Disclosure | number of instances | perception |
|---|---|---|
| true location | 17 | 13 true, 4 fairly true |
| true location with activity | 6 | 5 true, 1 fairly true |
| false location | 2 | fairly true |
| false location with activity | 4 | 1 true, 3 fairly true |
| Blurring | 6 | 2 true, 4 fairly true |

The main issues discovered during the pilot study had to do with a relatively steep learning curve for one of the participants, who was not familiar with the Nokia platform. This resulted in occasional delay by that participant in sending requests out to the others. The look and feel of the Mobile Client interface changes with the underlying platform. The said participant was taken through the use of the Mobile Client on the Nokia platform in order to facilitate its use in the main user study.

Another issue encountered by participants during the pilot study was that Mobile Client did not run all the time on participants' mobile devices. This led to:

- Location requests and disclosures not received at all.
- Delayed responses.

In order to address the above issues, participants were told to verify that the Mobile Client application was running on their phones at least three times a day. These reminders were sent via the Mobile Client at 7am, 1pm, and 7pm everyday during the main study.

**User Study:** 2 weeks

The main study was carried out over a two week period. Roles were assigned to participants, either 'requestor' or 'discloser', with two participants in each role. This was deliberate in order to limit to the disclosures the specific knowledge of the disclosure strategies and of whether the day required true locations or false locations. Each day, participants were sent an alert as to what task they were to carry out that day. Each requestor was asked to make at least one request per weekday (out of school hours) and a maximum of three requests per day at weekends. Each discloser was asked to use a particular disclosure strategy for any requests during that day: true location, true location with activity, false location, false location with activity, or blurred location. The reason for using one disclosure strategy per day was to avoid erratic answers arising from a change of strategy (e.g, true location alternating with false location). Automated daily alerts were sent via the Mobile

Feedback application. At the end of each day, participants were asked via Mobile Feedback how true the disclosures they received on that day were.

## 5.7 Data Capture and Analysis

Appendix D describes the type of data captured during each request/disclosure communication. Key data included the participant, the time of making a request, the type of intended disclosure (i.e. the disclosure strategy), the question posed to the requestor after a disclosure is made, and the response received from each requestor on their perceived believability of each disclosure.

The total number of valid disclosures collated at the end of the study was 70.

At the end of each day, a customized post-disclosure questionnaire was distributed to investigate the level of believability of each disclosure by the requestors. Post-disclosure data is found in Appendix D.

Responses were monitored and captured on Mobile Feedback and exported into an Excel spreadsheet for analysis. Each request was mapped onto the associated disclosure. Key data processed included the score for each response, the frequency of occurrence of a score, and the range of scores per technique per technique employed in a disclosure. Perception categories were mapped to values as in Table 5.3.

**Table 5.3:Score Represented by Perception of Disclosed Location to Requestor**

| Perception of disclosed location to requestor | Score |
|---|---|
| very true | 1 |
| True | 2 |
| fairly true | 3 |
| not true | 4 |

In order to understand how effective each technique was perceived, the mean and standard deviation of each disclosure technique employed were calculated as shown in Table 5.4. While we make no claims as to the statistical significance of the results, the mean perception score gives an indication of how truthful (closer to 1) or how deceitful (closer to 4) the technique was perceived as.

## 5.8 Findings

Figure 5.8-1 below is an illustration of perception of disclosures by requestors showing the minimum (most truthful) response and the mean response for each technique with the vertial line

showing the range of responses. The mean perception was lowest (considered most truthful) for responses with blurred location (score = 1). The figures indicate a low score for both the disclosure of a false location (1.21) and a blurred location. The mean perception of disclosures by requestors was highest for disclosures that included an activity, i.e. disclosing a true location with an activity (mean score of 1.5) and a false location and an activity (mean score of 2.78). The disclosure of a true location (with a mean score of 1.86) was perceived as being less truthful than a false disclosure as well as blurred location disclosure.

**Table 5.4: Mean Perception of Disclosure by Requestor**

| Technique | Response | Frequency | Score | Total Score | Total Frequency | Mean Score | Standard Deviation |
|---|---|---|---|---|---|---|---|
| False Location | Very True | 13 | 13x1=13 | 17 | 14 | 1.21 | 0.8018 |
| | True | N/A | N/A | | | | |
| | Fairly True | N/A | N/A | | | | |
| | Not True | 1 | 1x4=4 | | | | |
| False Location plus Activity | Very True | N/A | N/A | 39 | 14 | 2.78 | 0.5789 |
| | True | 4 | 4x2=8 | | | | |
| | Fairly True | 9 | 9x3=27 | | | | |
| | Not True | 1 | 4x1=4 | | | | |
| True Location plus Activity | Very True | 8 | 8x1=8 | 21 | 14 | 1.5 | 0.6504 |
| | True | 5 | 5x2=10 | | | | |
| | Fairly True | 1 | 3x1=3 | | | | |
| | Not True | N/A | N/A | | | | |
| True Location | Very True | 2 | 2x1=2 | 26 | 14 | 1.86 | 0.3631 |
| | True | 12 | 12x2=24 | | | | |
| | Fairly True | N/A | N/A | | | | |
| | Not True | N/A | N/A | | | | |
| Blurred Location | Very True | 14 | 14x1=14 | 14 | 14 | 1 | 0 |
| | True | N/A | N/A | | | | |
| | Fairly True | N/A | N/A | | | | |
| | Not True | N/A | N/A | | | | |

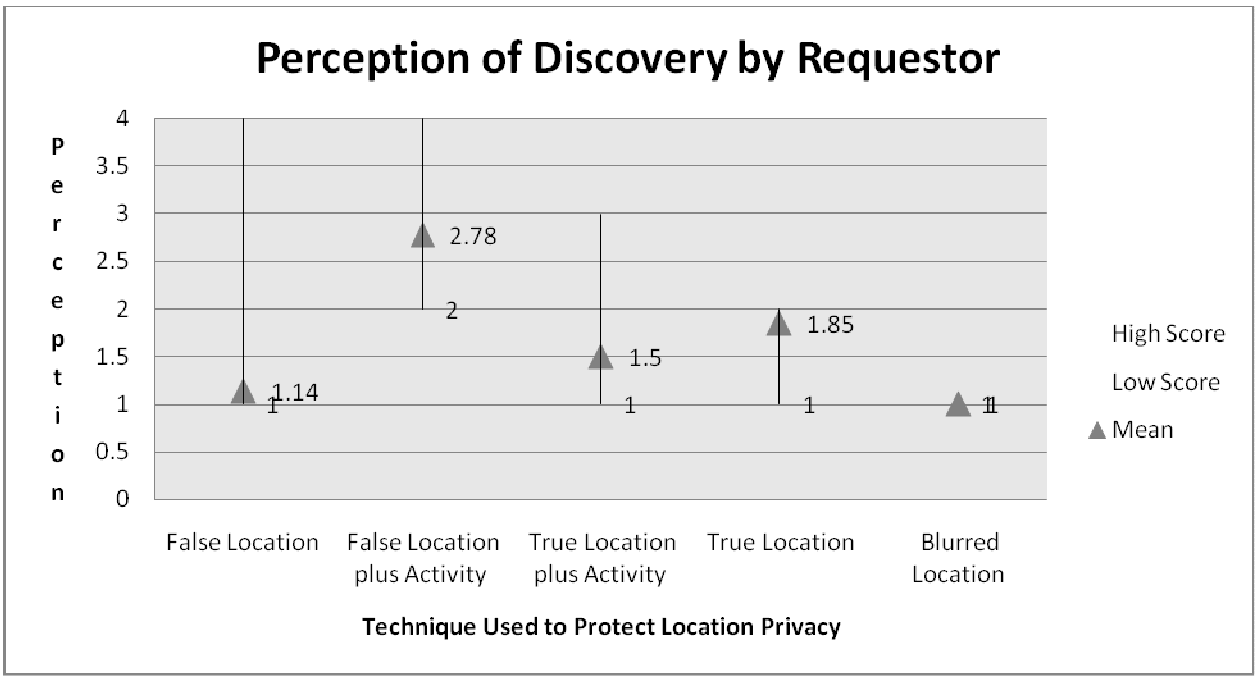


**Figure 5.8-1: Mean Perception of Disclosure by Requestor**

## 5.9 Threats to Validity

Some requests and disclosures were received on the native inbox instead of Mobile Client inbox. This led to some requests not being recorded. Hence, a reduction in total number of valid request/disclosure pairs may affect the validity of the evaluation process.

Threats to validity associated with the scale of the study have already been discussed above. A number of threats associate with the participants, in terms of cultural, gender or age bias, their competence with technology, the impact of their personal circumstances (e.g., the way age and attendance at school constrains their activity), and so on, apply. Similarly, threats may be associated with the tasks, and with the imposition of the artificial request/disclose regime. Further, the limitations of the current mobile phone technology, and the relative novelty of this sort of location disclosure, may also have an impact on behaviours. These are all matters to address in further work. However, the essence of this study was not to generalize but provide evidence of proof of concept that the Deception Privacy Control model is feasible.

## 5.10 Discussion

**The aim of the user study was to test the acceptability of reasonable deception in the field.** Although the low number of participants requires caution in generalizing from the results, two disclosure techniques showed potential for good control of location information: the disclosure of a plausibly false location and the disclosure of a blurred location.

**To what extent would people believe disclosures under different schemes?**
Contrary to what was anticipated, associating an activity with the location as a way of making false disclosures less easily detected, was not effective. The mean perception scores indicate that false location disclosures were perceived as more truthful than either true or false location disclosures plus activity. Although these findings are tentative, it appears that appending activity to a location disclosure raises suspicion, rather than enhancing disclosure plausibility.

**To what extent would members of a social group use personal knowledge in detecting deception?**
The post-study interviews made clear that both requestors and disclosers used personal knowledge, the latter in devising plausible false disclosures, and the former in interpreting the likely truthfulness of individual disclosures. For example, one requestor had this to say when asked of his perception of the veracity of a disclosure made to him:
*"I knew Adam was clearly not telling me his true location when he said he was in the club at about 10pm yesterday. Adam doesn't often do clubbing."*

**Would deception be detected or accepted in a genuine setting?**
This user study does not allow us to answer this fully. False disclosures were never detected in this study. Although the results do not rule out the possibility that deception might be detected, they do suggest that strong social bonds favour acceptance of plausible deception. A more comprehensive study (possibly an ethnographic study), including a variety of social networks, with varying strengths of social bond, would be required to investigate further.

## 5.11 Conclusion

In this chapter, an integrated approach has been taken to provide empirical validation of the ability to effect a flexible control of location information. The study has provided evidence that intentional blurring and false location disclosures are effective in withholding location as a means of protecting location privacy.

The study also shows that gathering data using mobile telephony can be a useful way of providing rich data in the field for usability research in the mobile environment.

In conclusion, two techniques employed in the Mobile Client application have the potential to prove effective in the field. These are:

a. Intentionally providing **plausibly** false location information to the requester. The location presented needs to be convincing enough to serve the purpose of the distortion. The study showed that when this is done well enough, the recipient of the disclosed location tends to accept it as plausible.
b. The deliberate blurring of location information is effective in withholding location information, within the limits of this study.

It must be emphasized that no claims of generaliseability are made, as the sample size is not large enough to do so. The study provides a proof of concept of the practical implementation of the Deception Privacy Control model in the form of the Mobile Client application. An additional evaluation has been conducted to complement the field-based user evaluation. The next chapter describes a usability study of the Mobile Client application using Human Computer Interaction (HCI) experts as participants to investigate the usefulness and effectiveness of the functionality and principles upon which the deception-based privacy control model is based.

# *Chapter 6. Usability Evaluation of the Mobile Client Application*

## 6.1 Introduction

In this chapter, the Mobile Client (MC) application, based on the Deception-based Privacy Control (DPC) model described in Chapter 4, is evaluated from a usability perspective. The design of the MC was informed by the results of the two large scale studies described in Chapters 3 and 5. The MC was built as a prototype to facilitate the flexible disclosure of location using the techniques of deliberately withholding location information, blurring (i.e. proving coarse-grained location information), ambiguity, and outright false disclosure. Instantiating the DPC model into the MC application provides some guidance as to how the principles underpinning the DPC model can be realised practically. Therefore subjecting such an instantiation to a usability study informs the design of potential usability problems to be encountered in the use of the MC application. The study described in this chapter involves the use of human computer interaction experts in evaluating the functionality of the MC based on certain tasks provided to participants. The rest of the chapter presents the study, findings, and threats to the validity of the method employed.

## 6.2 Objectives of the study

The aim of carrying out a usability study is to demonstrate the usability of the MC application as an instantiation of the DPC model.

The key objective of this study was therefore to provide answers to the following question:

> *How usable is the Mobile Client application in its use of deception to control location privacy?*

To specifically answer the above question, a usability study of the MC prototype was carried out, the results of which are discussed in this chapter.

## 6.3 Methodology

The highly dynamic context-based use of location-based systems makes it difficult to evaluate their usability using conventional user evaluation techniques. Therefore field-based usability techniques

have become increasingly useful in evaluating location-based prototypes (Kjeldskov et al, 2003). Evaluation of mobile systems is still not as widely reported as that of web-based applications. However, in recent times the most common method of evaluating location-based systems and for that matter, mobile human-computer interaction, has been laboratory-based usability evaluations (Kjeldskov and Graham 2003).

In this study, I decided to employ a usability study because it involves conducting an evaluation of various tasks in the use of the MC application. The study was conducted in the laboratory environment as additional source of empirical validation to the initial field-based study conducted in Chapter five.

## 6.4 The Study

The study was conducted over a two week period. Six experts were involved. The composition of these participants is included:

a) 4 practicing HCI professionals each with a PhD qualification gained in the last 18 months (two females and two males).
b) 1 female senior lecturer and well-known HCI expert with a book to her credit.
c) 1 industry-leading female HCI expert.

In this study, no trials were carried out since the functionality of the MC application was evaluated during the user study in Chapter 5. Participants were taken through the use of the MC application after they had given their consent to take part in the study by filling in consent forms. The study was conducted in each participant's office on an individual basis.

**Table 6.1: Detailed Description of Tasks Used During Usability Study**

Imagine you and people in your social network have a location-tracking system (on your mobile phones) which may permit you to keep track of each other's location. People within your social network will typically include (but not limited to) friends, spouse/partner, colleagues, boss, and family. Imagine you are able to manipulate and control what location to reveal to whom, and at what time. Further imagine that you are able to disclose a location different from your true location using a privacy control feature that comes with the location tracking service. This gives you the ability not only to send an untrue location, but also to make the disclosed location look plausible enough for the requestor.

Using the Mobile Client application,

1. Add two contacts to the list of contacts including that provided by the study facilitator.
2. Set location disclosure preferences that you wish to employ for automatic disclosures for each contact
3. Select a contact and request for their location
4. You would receive a request from the study facilitator. Reply to this request by making a disclosure.
5. Delete a contact from the contacts list. This should be a contact other than the facilitator's details.

After stepping through each task, please record the usability problems you encountered, rating them as follows:

- A score of 0 corresponds to a situation where you think there is no usability problem in the particular task you are involved in.
- A cosmetic problem is rated a score of 1. This is given to usability problems that need not be fixed unless there is extra time for fixing such problems.
- Minor usability problems should have a score or rating of 2. These are low priority problems but need to be fixed when deciding to fix usability issues.
- Major usability problems (rated 3) should be given high priority and hence, should be fixed.
- Severe usability problems, also called catastrophic usability problems must be fixed before the product is released. These problems are rated 4.

## 6.5 Data Capture and Analysis

Each participant was given a form to fill in during each task. The form basically provided fields for participants to state usability problems identified and their severity ratings as described in Table 6-1 above.

During the study, the participants were engaged in a discussion on each scenario where clarification was required. This also provided an additional source of information for use in the overall analysis. Participants were also given the option to rate the usefulness of the prototype in

general in the control of location privacy. The essence of this was to provide some kind of corroboration with the field-based study described in Chapter five.

Problems identified for each task were analysed to determine the existence of a pattern across the participants. These patterns are described in the next sections. Analysis of responses was based on Nielson's (1994) recommendations in his work. These are: the *frequency* of occurrence of each problem, the *impact* (severity rating) of the problem and *persistence* of the problem (i.e. whether users will repeatedly be bothered by such problems).

## 6.6 Findings

In total, 58 usability problems were discovered as shown in Table 6-2 below. These problems were rated in accordance with Nielsen's (1994) ratings for usability studies.

a) A score of "0" corresponds to a situation where participants think there is no usability problem in the particular task they were involved in.
b) A cosmetic problem is rated a score of "1". This is given to usability problems that need not be fixed unless there is extra time for fixing such problems.
c) Minor usability problems should have a score or rating of "2". These are low priority problems but need to be fixed when deciding to fix usability issues.
d) Major usability problems (rated 3) should be given high priority and hence, should be fixed.
e) Severe usability problems, also called catastrophic usability problems must be fixed before the product is released. These problems are rated 4.

**Table 6.2: No. of Usability Problems Identified by each Participant for each Problem Classification**

| | **Participant 1** | **Participant 2** | **Participant 3** | **Participant 4** | **Participant 5** | **Participant 6** | **Total** |
|---|---|---|---|---|---|---|---|
| **Severe** | - | 4 | 3 | 3 | - | 1 | 11 |
| **Major** | 3 | 2 | 1 | 3 | 2 | 12 | 23 |
| **Minor** | 3 | 2 | 5 | 5 | 2 | 2 | 19 |
| **Cosmetic** | - | 1 | 1 | 2 | 1 | - | 5 |
| **Total** | **6** | **9** | **10** | **13** | **5** | **15** | **58** |

Figure 6.6-1 below illustrates the distribution of severity of usability problems presented in Table 6.2 above. The figure indicates that most usability problems are major and minor in severity (42) whilst only 16 problems discovered are either severe or cosmetic.

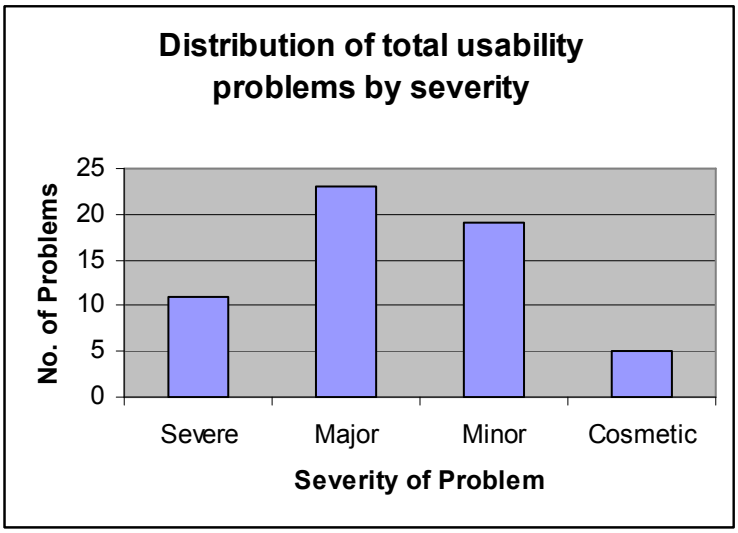


**Figure 6.6-1: Distribution of Total Usability Problems by Severity**

Note that in Table 6.2 above, zero-score usability problems have not been included for two main reasons. Firstly, they present no challenges for further discussion. Furthermore, within the given limits of the mobile platform available most zero-score issues were platform related and hence, did not have a direct relationship with the model upon which the MC application is based.
In the next sections, a distillation of the above table into the various tasks is described in more detail.

**Table 6.3: No. of All Usability Problems Identified by Each Participant for Each Task Performed**

| Participant / Task | Participant 1 | Participant 2 | Participant 3 | Participant 4 | Participant 5 | Participant 6 | Total |
|---|---|---|---|---|---|---|---|
| **Adding Contacts** | 2 (33.33%) | 4 (44.44%) | 4 (40%) | 3 (23.07%) | 1 (20%) | 2 (13.33%) | 16 |
| **Preference Setting** | 1 (16.67%) | 1 (11.11) | 1 (10%) | 4 (30.77%) | 2 (40%) | 4 (26.66%) | 13 |
| **Making a Request** | - | 2 (22.22%) | 1(10%) | 3 (23.07%) | - | 4 (26.66%) | 10 |
| **Making a Disclosure** | 3 (50%) | - | 2 (20%) | 2 (15.38%) | - | 4 (26.66%) | 11 |
| **Delete Contact** | - | 1 (11.11%) | 1 (20%) | - | - | 1 (6.67%) | 3 |
| **Error Handling** | - | - | - | - | 1 (20%) | - | 1 |
| **Other** | - | 1 (11.11%) | 1 (10%) | 1 (7.69%) | 1 (20%) | - | 4 |
| **Total** | **6** | **9** | **10** | **13** | **5** | **15** | **58** |

### 6.6.1 Adding Contacts

All six participants discovered usability problems in this task. These ranged from minor to severe. There were no cosmetic problems recorded by all six participants in the task of adding contacts. Table 6.4 below shows the breakdown of problems discovered by all participants in this task.

**Table 6.4: No. of Usability Problems Discovered by Severity During Contact Addition**

| Severity | Cosmetic | Minor | Major | Severe | Total |
|---|---|---|---|---|---|
| No. of problems | 0 | 5 | 4 | 7 | 16 |

In this task, the problems discovered can be categorized into three main areas, namely,

1. Problems related to synchronizing contacts with native phonebook entries. For instance, participant 6 said this when she undertook the task of adding contacts: *I am not able to load contacts from my phonebook. Currently, the application only allows me to import contact numbers from the phonebook once I enter the user's name. It'll be good to have a one-off import of both name and number from the phonebook.*
2. Unable to edit contacts. Participant 3 said this of the task of adding contacts: *I have just made a mistake in entering a contact's number. MC does not allow me to edit the contact's details. It'll be a good idea to be able to edit any contact details at any time of the use of MC.*
3. Navigation problems in the contacts capture form. Participant 2 had this to say during the add contacts task: *In the contacts form, I can't get back to the contacts list. Perhaps adding a **back** button to **options** will be useful.*

**Table 6.5: No. of Usability Problems According to the Nature of Problem During the Task of Adding Contacts**

| **Nature of usability problem** | **No. of problems encountered** |
|---|---|
| Phonebook synchronization | 5 |
| Unable to edit contacts | 2 |
| Navigation problems in contacts capture form | 9 |
| Total | 16 |

From the above table, majority of the problems (56.25%) were navigation problems within the contacts capture form. Four out of the six participants discovered these. The least number of problems discovered came from the lack of the ability to edit contacts (only two problems discovered).

### 6.6.2 Setting of Disclosure Preferences

Thirteen usability problems were discovered in the task of setting disclosure preferences with severity between minor and severe, as shown below. As in the task of addition of contacts, there were no cosmetic usability problems recorded in this task.

**Table 6.6: No. of Usability Problems Discovered by Severity During the Task of Disclosure Preference Setting**

| Severity | Cosmetic | Minor | Major | Severe | Total |
|---|---|---|---|---|---|
| No. of problems | 0 | 6 | 4 | 3 | 13 |

Three key problems discovered during this task were:

1. The lack of a clear visibility between the preference set and the relevant contact to whom the preference is applied. For instance, participant 6 described this problem by saying: *There is a clear lack of affordance in the preference setting task as there is no indication of the action that has been taken. That is, I'm not able to know at a glance whose preference I'm about to set.*
   Similarly participant 1 said this of the same problem: *preferences should have clarity as who they apply to.*
2. Navigation problems with the preference setting form. Participant 2 paraphrases this problem in these words: *Getting out of the preference form is not easy to tell as the **back** button is missing. Some kind of **options** button will also be useful here.*
3. The lack of flexibility in setting other preferences. Here, participant 4 had this to say: *The application should provide enough flexibility to set preferences. For instance, there should be a preference option where one can select all contacts on a particular day (such as a day I'm in a meeting at the MoD) and disclose a false location.*

**Table 6.7: No. of Usability Problems According to the Nature of Problem During the Task of Setting Disclosure Preferences**

| **Nature of usability problem** | **No. of problems encountered** |
|---|---|
| The lack of a clear visibility between the preference set and the relevant contact to whom the preference is applied | 6 |
| Navigation problems with the preference setting form | 3 |
| The lack of flexibility in setting other preferences | 4 |
| Total | 13 |

46.15% of the usability problems resulted from the lack of clear visibility between the setting of preferences and the relevant contact to whom the preference is applied (see Table 6.7 above). Four of the six participants discovered these.

### 6.6.3 Making a Location Request

Seven usability problems were discovered in the task of setting disclosure preferences with severity between minor and severe, as shown below.

**Table 6.8: No. of Usability Problems Discovered by Severity During the Task of Making a Location Request**

| Severity | Cosmetic | Minor | Major | Severe | Total |
|---|---|---|---|---|---|
| No. of problems | 0 | 6 | 3 | 1 | 10 |

Two key problems discovered during this task were :

1. Issues with request notification including too short request feedback timeframe. Participant 1 said: *Since I do not remember phone numbers that easily, it'll be good to have the message alert include the name of the contact rather than the contact number.*
2. The lack of flexibility in making requests such as tagging of a request to include its nature, e.g. requests requiring urgent attention no matter what. Participant 1 in particular had this to say: *Since my ability to respond to a location request depends on the context of the request, I'll be interested in how urgent the request is and whether I can wait and respond when I'm less busy. Hence, some kind of tagging of a request will be a great enhancement to this application.*

**Table 6.9: No. of Usability Problems According to the Nature of Problem During the Task of Making a Location Request**

| **Nature of usability problem** | **No. of problems encountered** |
|---|---|
| Issues with request notification including too short request feedback timeframe | 8 |
| The lack of flexibility in making requests such as tagging of a request to include its nature, e.g. requests requiring urgent attention no matter what | 2 |

### 6.6.4 Making a Location Disclosure

Seven usability problems were discovered in the task of setting making a disclosure with severity between cosmetic and severe, as shown below.

**Table 6.10: No. of Usability Problems Discovered by Severity During the Task of Making a Location Disclosure**

| Severity | Cosmetic | Minor | Major | Severe | Total |
|---|---|---|---|---|---|
| No. of problems | 1 | 4 | 5 | 1 | 11 |

Two key problems discovered during this task were:

1. Disclosure notification problems. Participants either found the disclosure notification message to be too wordy or lacked completeness. For instance, participant 1 said this: *Though I find this method of disclosure appropriate, users could benefit by making sense of the time the disclosure was made. This in my opinion, is not major in terms of severity.*
2. Disclosure feedback issues. Participant 2 said of this task: *I do not remember the disclosure I just made and I'm not able to tell whether I disclosed what I had in mind or not. This is where it'll be useful including the disclosed location in the disclosure alert.*

**Table 6.11: No. of Usability Problems According to the Nature of Problem During the Task of Making a Location Disclosure**

| **Nature of usability problem** | **No. of problems encountered** |
|---|---|
| Disclosure notification problems | 5 |
| Disclosure feedback issues | 6 |

### *6.6.5 Deleting a contact*

Only three problems were recorded by participants during this task. Whilst two participants perceived the lack of a clear delete warning to be of minor severity, one participant clearly saw it as a severe usability problem.

**Table 6.12: No. of Usability Problems Discovered by Severity During the Task of Deleting a Contact**

| Severity | Cosmetic | Minor | Major | Severe | Total |
|---|---|---|---|---|---|
| No. of problems | 0 | 2 | 0 | 1 | 3 |

The main usability problem discovered in a delete contact task was the absence of a warning prior to deleting a contact in the contact list. One participant (participant 6) had this to say: *I just tried deleting a contact and I was not warned as to whether I indeed wanted to delete the contact or not. This is definitely a catastrophic usability problem.*

**Table 6.13: No. of Usability Problems According to the Nature of Problem During the Task of Deleting a Contact**

| Nature of usability problem | No. of problems encountered |
|---|---|
| Delete Warning | 3 |

### *6.6.6 Error Handling*

Only one usability problem was recorded during the whole exercise. In this case participants were required to look out for errors and rate their severity.

**Table 6.14: No. of Usability Problems Discovered by Severity During the Task of Error Handling Evaluation**

| Severity | Cosmetic | Minor | Major | Severe | Total |
|---|---|---|---|---|---|
| No. of problems | 0 | 0 | 1 | 0 | 1 |

**Table 6.15: No. of Usability Problems According to the Nature of Problem During the Task of Error Handling Evaluation**

| Nature of usability problem | No. of problems encountered |
|---|---|
| Duplication of disclosure message when making a disclosure to a second request | 1 |

## 6.7 Platform Problems

In this study, a number of issues were raised by participants which had nothing to do with the MC application as a whole but just the Nokia platform. One participant (participant 1) who is an expert in the evaluation of mobile systems in particular, clearly discovered less problems (5 problems in all) than the rest of the participants. This section outlines the platform problems that were not considered in the scope of this study.

The MC application needs to be on all the time for requests and disclosures to be made during interactions. The application was tested using a Nokia 6600. On this platform, when another program is started whilst MC is in use, the MC application automatically runs in the background, allowing the user to be able to receive requests uninterrupted. Participants in this study used the Nokia N90 which did not allow MC to run in the background, and as such the MC application always closed when another application interrupted it, such as a phone call or navigating away from the MC application. All the participants but one saw this to be a usability problem. However, participant 1 (who has knowledge of mobile platforms) disagreed and explained that mobile applications have always faced such interaction problems because platform pervasiveness is still a major issue of concern in mobile computing.

Another platform related problem was a generic message alert that is automatically generated to confirm sending a text message. This is a security feature in current mobile platforms that prevent sending programs without user intervention. It is the same feature that is used to prevent spreading viruses in mobile platforms. Hence, considering such alerts as usability problems was discounted from the study, clearly separating what is a platform problem from typical usability issues bothering the design of applications for the mobile environment.

## 6.8 Threat to Validity

The participants' knowledge of the particular mobile platform may have influenced navigation of the MC environment. Whilst one participant saw issues such as request feedback and notification as platform related usability problems, the others thought they were problems introduced by the MC application. This indeed, is a threat to the validity of the study. However, most participants were able to correctly identify application related usability problems, and that is what the conclusions of this study are based on.

## 6.9 Discussions

My results show that most problems came from contact addition tasks. The findings in this study provide guidance to the design of usable privacy control interfaces on the mobile platform. The most common usability problem in this task had to do with navigation in the contacts capture form. Then the next problem of concern to participants was request notification which also included the short request feedback timeframe.

Then the lack of a clear visibility between the set preference and the relevant contact to whom a preference is applied was the next usability problem of concern to participants. This was equally as important as phonebook synchronization with the contacts list.

The rest of the usability problems were discovered by at most four participants thus, recording a low frequency. In order of frequency of occurrence, here is a list of all the issues discovered during the exercise.

1. Navigation problems in contacts capture form.
2. Issues with request notification including too short request feedback timeframe.
    - The lack of a clear visibility between the preference set and the relevant contact to whom the preference is applied.
3. Phonebook synchronization.

- Disclosure feedback issues.

4. The lack of flexibility in setting other preferences.
    - Disclosure notification problems.
    - Delete Warning.
5. Navigation problems with the preference setting form.
    - Unable to edit contacts.
6. Duplication of disclosure message when making a disclosure to a second request.
    - The lack of flexibility in making requests such as tagging of a request to include its nature, e.g. requests requiring urgent attention no matter what.

## 6.10 Conclusion

In this study, I have provided empirical validation of the ability to effect a flexible control of location information. This corroborates with earlier results from the field-based study, which demonstrates the feasibility and effectiveness of the use of the mobile platform in location privacy control.

a. In conclusion, the study shows that effective design of location privacy systems depends on two key factors. The provision of clear and easy to navigate interfaces for each task to be carried out in a request/disclosure flow process.
b. The ability to mimic existing patterns of use of common tasks associated with mobile platforms, such as instant messaging, contacts addition, feedback, etc.

# *Chapter 7. Conclusions*

## 7.1 Introduction

In a networked world, user choice regarding what to disclose to whom is often complicated (Palen & Dourish, 2003). *Context* as emphasised by Adams (1999) helps frame behaviour (Harrison & Dourish, 1996). However, the sense of place (as a context), rather than space, determines behaviour (Harrison & Dourish, 1996). In this research, we argued user location, described as the sense of place, impacts social behaviour. In social interactions, the perception of users about who has access to their location and to what extent location is disclosed, is particularly very important because such location information is related to "*socially determined notions of the individual within society"* (Adams, 1999; Goffman, 1959; Agre, 1997). Therefore the scope of this thesis has been limited to the notion of privacy related to user location.

Location privacy has in recent times become an issue of concern to privacy conscious users of mobile devices. As social tools, most of these mobile devices (mobile phones to be specific) are not built to provide the flexible control of the location of users of applications that take into account real-time user locations. By incorporating some social practices such as deception (whether explicit or intentional blurring), I contribute to better and more effective user control of the amount of real-time location information users wish to disclose.

By conducting online scenario-based exploratory studies, I was able to investigate the popularity of the use of deliberate withholding of information (called *deception*) among a large cross section of online participants. Having been certain of the high percentage of respondents willing to employ some kind of deception to protect their location privacy, mostly for good reasons, I proposed and designed a deception-based privacy control model. An instantiation of the model in the form of the Mobile Client (MC) application was evaluated in two different perspectives – a user study and an expert usability study. The aim of these evaluations was to provide validation of the usefulness of the model in protecting location privacy. The results of the user evaluation shows the superiority of intentional blurring as a location privacy protection technique over outright deception. The usability evaluation was done on the prototype to investigate its usability using various tasks. A usability evaluation is a much quicker way of evaluating the usability of such prototypes using well-designed scenarios.

## 7.2 Goals & Findings

This thesis has provided a knowledge base contribution to the mobile HCI research community in two ways:

**a. Model Findings**

An exploratory DPC model of user control of location privacy has been developed. The model encapsulates a five-layer disclosure approach and two disclosure strategies of mis-direction and ambiguity. Empirical studies in the field revealed that disclosing a plausibly false location will be difficult to detect as being false. This strategy will inform the design of disclosure mechanisms in situations which demand the deliberate withholding of location information as a way of preserving privacy.

The model also showed from field studies that blurring (i.e. intentionally regulating the accuracy of location information disclosed) can be a good design consideration in the control of location privacy.

**b. Methodological Findings**

This thesis has provided an empirical approach in its methodology. The DPC model was investigated using a field-based empirical study. The importance of using scenarios in an exploratory design has already been articulated in Chapter 4.

## 7.3 Critical Review of Thesis

Two key limitations can be leveled against this thesis. These include a limitation in:

a) Scope, and

b) Methodology

In the next two sections these limitations are presented in detail.

### *7.3.1 Scope*

This thesis has been limited by its scope to:

i. Privacy resulting from location disclosure rather than privacy in other environments such as sensor environments.

ii. Peer-to-peer communications between people of same social networks rather than communications involving the disclosure of location information to third parties such as retail shops and government agencies.

The limited scope of the thesis may suggest that its findings are limited too. However, the context-specific definition of privacy makes it appropriate to provide a focused and in-depth study of privacy in this context. Despite the lack of large scale empirical studies in location disclosure, the findings of this research very useful in the following ways:

a. The findings provide some pointers to location privacy system designers of what techniques may be useful in preserving privacy.

b. The findings also add to the common body of knowledge in the mobile HCI environment as well as an emerging social mobile computing field (Smith et al, 2005).

### *7.3.2 Methodology*

The use of a small sample size for the field-based user study may seem to be unrepresentative of the entire user population. However, the purpose of the evaluation was not to gather data to make a generalization, but as proof of concept of the DPC model.

The DPC model was implemented using Java for mobile devices (J2ME). One may argue that not all mobile phones are java-enabled. However, there is an increasing trend of newer mobile phones becoming java-compliant. Besides, building the DPC model was a proof of concept. Hence, having proved that the DPC model can be implemented practically, it should not be difficult to design the model on other platforms.

## 7.4 Contributions

This research contributes to the common body of knowledge in the area of location privacy and demonstrates how established social practices can effectively support technology. In particular, the main contribution of this research is aimed at providing a flexible location disclosure through the use of an established social practice - the deliberate withholding of location information to protect one's privacy (called *deception* in this work).

As a recap from Chapter one, the key research question includes the following:

*How can privacy needs be balanced with location sharing in mobile computing?*

1. What techniques can be used to protect location privacy?
2. To what extent can deception be used to protect location privacy?
3. What factors influence the use of deception to protect location privacy?
4. How can deception be implemented in social mobile computing?

To start with, exploratory evidence in the literature (Section 1.2) has provided the case for a privacy concern in the use of location-based services and techniques used to protect location privacy as discussed in Chapter 2 (refer to research sub-question1 above).

The main contribution of this research is the re-contextualisation of deception from social psychology and information systems security to the field of location privacy. I am among the first to provide empirical evidence that deception is an appropriate technique for protecting location privacy. This was done by conducting a large scale scenario-based online study to investigate how likely participants were to use deception as a location privacy protection technique. In addition, I have conducted usability studies to examine suitability, usefulness and effectiveness of a deception-based privacy control model. These studies have provided, within the limits of the research, evidence of the extent to which deception can be used to protect location privacy (research sub-question 2 above).

I have also provided empirical evidence in this work to explain the high level of discomfort in the use of deception as a technique. In particular, evidence suggests that the possibility of deception detection is related to the level of discomfort. That is, a higher possibility of discovery or detection suggests a higher the level of discomfort in the use of deception. Evidence in this research suggests that likelihood and discomfort are key factors affecting the use of deception to control location privacy (research sub-question 3).

In the user validation, two disclosure techniques showed the potential for good control of location information. These are: the disclosure of a plausibly false location and the disclosure of a blurred location. These were seen to be more effective in carrying the message behind the disclosures across to requestors.

The usability study revealed that effective design of location privacy systems depends on two key factors:

a) The provision of clear and easy to navigate interfaces for each task to be carried out in a request/disclosure flow process.
b) The ability to mimic existing patterns of use of common tasks associated with mobile platforms, such as instant messaging, contacts addition, feedback, etc.

In short, the contributions of this thesis can be summed up as:

1. Empirical evidence that deception is good for controlling location disclosure, and therefore location privacy.
2. A deception-based privacy control model depicting how deception can be implemented in social mobile computing (providing answers to research sub-question 4).
3. Empirical evidence of the effectiveness of this model in controlling location disclosure.

## 7.5 Future Work

I recommend further work in a number of areas in order to provide a complete and end-to-end location privacy protection system. First, a prototype built with full location capturing capability will help improve data quality in the evaluation process. The next stage of this work is to incorporate deception preferences into a privacy preference model for location-based applications in a platform-independent environment. Since most smart phones now are Java -enabled, such a preference model needs to take advantage of this to leverage the flexibility that comes with object-oriented programming. By encapsulating privacy preferences in a mobile agent (Yamada & Kamioka, 2005, and Adam, K et al, 2005), privacy preference negotiations can easily be done to preserve individual privacy settings of people within a social network, while disclosing just the amount of location information required by each requestor.

A challenging issue is to examine how the deliberate withholding of location information can be effective in a dynamically changing context. This is particularly useful in situations where disclosure preferences have been set for each contact person for particular contexts. If contexts change frequently (such as every hour), a key challenge will be to determine when to withhold location information and when to disclose a true location based on a rapidly changing context.

The DPC model is not context-dependent in terms of location, activity and time. It is only based on location as an assumption of activity. For instance, it pre-supposes that being in a gift shop means one is intending to buy a gift. The person could be seeing or meeting a friend at the shop, or doing something else other than buying a gift.

An interesting research problem is to study the accuracy of context inference from location information. Context in this case should mean an encapsulation of location, time, and activity.

In conclusion, I plan to implement the new DPC model (taking into account the outcome of the usability study) on different mobile phone platforms and repeat the field-based study on a large scale. This will help minimize any biases or threats to validity in the first study. It will also be interesting to find out if the fact that participants knew that they were involved in a study may have influenced the outcome. Using real life data will help boost the validity of the DPC model.

# References


Abowd, G.D., Mynatt, E.D. (2000). *Charting past, present, and future research in ubiquitous computing.*ACM Trans. Comput.-Hum. Interact. 7(1): 29-58.

Ackerman, M. S. (2004). *Privacy in pervasive environments: next generation labeling protocols*. Personal Ubiquitous Computing, *8*( 6), 430-439.

Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification*. Paper presented at the 5th ACM conference on Electronic commerce, 21-29.

Adam, K., Price, B., Richards, M., & Nuseibeh, B. (2005). *A Privacy Preference Model for Pervasive Computing.* Paper presented at the The First European Conference on Mobile Government, University of Sussex, Brighton, 10-12 July.

Adams, A (2001). *Users' perceptions of privacy in multimedia communications.* Unpublished PhD thesis, school of psychology, University College London, 30-31.

Adams, A. (1999). *The implications of users' privacy perception on communication and information privacy*. In Proceedings of the Telecommunications Policy Research Conference (Washington, DC).

Agre, P.E. (1997). *Computation and human experience*, Cambridge University Press, Cambridge.

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks/Cole.

Aquinas, T. (1947). *Summa Theologica* (F. o. t. E. D. Province, Trans.), 2–2, 110, 3c.

Aristotle. (350 BC). *Nicomachean Ethics.* (W. D. Ross, Trans.).

AT&T. (2003). *Privacy Bird*, available from: http://www.privacybird.com

AT&T. (2004). *Find People Nearby*. Retrieved 31 January, 2005, available from: http://www.attwireless.com/personal/features/organization/findfriends.jhtml

Augustine. (1952). *Lying & Against Lying*. In R. J. Deferrari (Ed.), Treatises on Various Subjects (Vol. 14, 16). New York: Catholic University Press.

Augustine. (1961). *Enchiridion, On Faith, Hope and Love*. Chicago: Henry Regnery Company.

Barkhuus, L.& Dey, A. (2003). *Location-Based Services for Mobile Telephony: A Study of User's Privacy Concerns.* Paper presented at the INTERACT, 9th IFIP TC13 International Conference on Human-Computer Interaction, July, 709-712.

Bellotti, V., Sellen, A. (1993). *Design for Privacy in Ubiquitous Computing Environments.* In: Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93), Kluwer 77–92

Benford, S., Seager, W., Flintham, M., Anastasi, R., Rowland, D., Humble, J., Stanton, D., Bowers, J., Tanadavanitj, N., Adams, M., Farr, J. R., Oldroyd, A., & Sutton, J. (2004). *The Error of Our*

*Ways: The Experience of Self-Reported Position in a Location-Based Game.* Paper presented at the Ubicomp 2004, 70-87.

Beresford, A. R., & Stajano, F. (2003). *Location Privacy in Pervasive Computing.* IEEE Pervasive Computing, *2*(1), 46-55.

Berg Insight. (2006). *LBS 2006 Temperature Meter*. available from: http://www.lbsinsight.com/filearchive/4/417/LBS%20Insight%20Survey%202006.pdf

Black, E. (2001). *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation*. New York: Crown.

Bok, S. (1978). *Lying: Moral Choice in Public and Private Life*: The Harvester Press.

Boyle, M. (2003). *A Shared Vocabulary for Privacy.* Paper presented at the Fifth International Conference on Ubiquitous Computing, Seattle, Washington, October 12-15, 2003.

Caddell, J. (2004). *Deception 101—Primer on Deception*. US Army War College.

Carroll, J.M. (2000) *Five reasons for scenario-based design, Interacting with Computers,* 13(1), 43-60. (http://www.sciencedirect.com/science/article/B6V0D-4106B52-3/2/95237a4cc44e018d730065eb2724b623)

Cavoukian, A. (2004). *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*: Information and Privacy Commissioner of Ontario. available from: http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=15007

Christian, D., & Young, R. M. (2004). *Strategic Deception in Agents.* Paper presented at the AAMAS-04 Workshop on Learning and Evolution in Agent Based Systems, New York.

Christian, F., Roland Schneider, & Langheinrich, M. (2004). *Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols.* Paper presented at the 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), Tokyo, Japan, November 2004.

Clements, B., Maghiros, I., Beslay, L., Centeno, C., Punie, Y., Rodriguez, C., & Masera, M. (2003). *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview* (EUR 20823 EN). available from: ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf

Cohen, F., Lambert, D., Preston, C., Berry, N., Stewart, C., & Thomas, E. *A Framework for Deception*. Retrieved 08/07/2005, available from: http://all.net/journal/deception/Framework/Framework.html

Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). *Location Disclosure to Social Relations: Why, When, & What People Want to Share.* Paper presented at the Conference on Human Factors in Computing Systems, CHI 2005, Portland, Oregon, USA, 81-90..

Corby, J. M. (2002). *The Case for Privacy*. Information systems security, *11*(2), 9 - 14.

Cranor, L. (2002). *Web Privacy with P3P*. Cambridge, MA: O'Reilly & Associates.

Daniel, D., & Herbig, K. (1982). *Strategic Military Deception (Pergamon Policy Studies on Security Affairs)*. Pergamon Pr.

DePaulo, B. M., & Kashy, D. A. (1998). *Everyday Lies in Close and Casual Relationships*. Personality and Social Psychology Bulletin, *74*(1), 63–79.

Detlev Zwick & Nikhilesh Dholakia (1999). *Models of privacy in the digital age: Implications for marketing and e-commerce.* http://ritim.cba.uri.edu/Working%20Papers/Privacy-Models-Paper%5B1%5D.pdf

Duckham, M., & Kulik, L. (2005). *A formal model of obfuscation and negotiation for location privacy.* Paper presented at the 3rd Int'l Conf on Pervasive Computing: Pervasive '05, Munich, Germany, 8-13 May, 152-170.

Duckham, M., Mason, K., Stell, J., & Worboys, M. (2001). *A formal approach to imperfection in geographic information.* Computers, Environment and Urban Systems, *25*, 89–103.

Dunne, C. R., Candebat, T., and Gray, D. (2008). *A frequency based sighting blurring algorithm for use with location based services on the internet*. In Proceedings of the 10th international Conference on Human Computer interaction with Mobile Devices and Services (Amsterdam, The Netherlands, September 02 - 05, 2008). MobileHCI '08. ACM, New York, NY, 3-12. DOI= http://doi.acm.org/10.1145/1409240.1409242

Dwyer, J., Hrubes, D., & Signorile, E. (2004). *Gender Differences in the Use of Emotion-Focused Deception*, available from: http://profweb.ws/~daniel.hrubes/EPApresentationjen.pps#256,1, Gender Differences in the Use of Emotion-Focused Deception.

Ellis, H. S., & Fellner, W. (1943). *External Economies and Diseconomies.* American Economic Review, *33*, 493-511.

EPIC. (2002). *Privacy and Human Rights 2002 An International Survey of Privacy Laws and Developments*. available from: http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf

EPIC. (2003). *Privacy and Human Rights 2003: Overview*. Retrieved 29/04/2005, available from: http://www.privacyinternational.org/survey/phr2003/overview.htm#Defining%20Privacy

Esler, M., Hightower, J., Anderson, T., and Borriello, G. (1999). *Next century challenges:*

*Data-centric networking for invisible computing*. In Proceedings of MobiCom'99, Seattle.

EU. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, available from: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Fléchais, I. (2005). *Designing Secure and Usable Systems*. PhD thesis, University College London.

Gavison, R. (1984). *Privacy and the limits of law*. In F. Schoeman (Ed.), Philosophical Dimensions of Privacy: An Anthology. New York, NY: Cambridge University Press.

Globallocate. *Everything you want to know about E911 and E112*. Retrieved 21/04/2005, available from: http://www.globallocate.com/RESOURCES/RESOURCES_MAIN_f3.htm

Goffman, E. (1959). *The Presentation of Self in Everyday Life.* (Reprinted ed.): Penguin Books, 1990.

Gordon, S. (2003). *Privacy: A Study of Attitudes and Behaviors in US, UK and EU Information Security Professionals*, Retrieved on 7/11/2008, available from: http://securityresponse.symantec.com/avcenter/reference/privacy.attitudes.behaviors.pdf

Grinter, R. E. and Eldridge, M. (2001). *y do tngrs luv 2 txt msg&quest*. In Proceedings of the 7th European Conference on Computer-Supported Cooperative Work (ECSCW). Bonn, Germany (Sept. 16--20). 219-238

Gross, T., & Specht, M. (2001). *Awareness in Context-Aware Information Systems.* Paper presented at the Mensch & Computer - 1. Fachübergreifende Konferenz, Bad Honnef (Germany), 173-182.

Gruteser, M., & Grunwald, D. (2003). *Anonymous usage of Location-Based Services Through Spatial and Temporal Cloaking.* Paper presented at the First International Conference on Mobile Systems, Applications, and Services.

Gunter, C. A., May, M. J., & Stubblebine, S. G. (2004). *A Formal Privacy System and its Application to Location Based Services.* Paper presented at the Workshop on Privacy Enhancing Technologies, Toronto, Canada.

Gunter, C. A., Wachter, S., & Wagner, P. (2004). *Location-Based Services in the Privacy Matrix*, available from: http://www.spatial.maine.edu/~nittel/lp/gunter_abstract.pdf

Hancock, J. T., Thom-Santelli, J., & Ritchie, T. (2004). *Deception and design: the impact of communication technology on lying behavior.* Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems table of contents, Vienna, Austria, 129 - 134.

Harrison, S. & Dourish, P. (1996). *Re-place-ing space: the roles of place and space in collaborative systems*. Paper presented at the Proceedings of the 1996 ACM conference on Computer supported cooperative work, Pages: 67-76**,** Boston, Massachusetts, United States.

Harper, D. (2001). *Online Etymology Dictionary*, available from: http://www.etymonline.com/index.php

Hassan, Riffat (1996). *Religious Human Rights in the Qur'an*. Available from http://muslim-canada.org/emory.htm Retrieved on 2008-03-04.

Hixson, R. (1987). *Privacy in a Public Society: Human Rights in Conflict 3*: Oxford Univ Press.

Höflich, J.R., Rössler, P. (2001). *Mobile schriftliche Kommunikation oder: E-Mail für das Handy*, Medien & Kommunikationswissenschaft*,* Vol. 49 pp.437-61.

Hong, J. I., & Landay, J. A. (2004). *An Architecture for Privacy-Sensitive Ubiquitous Computing.* Paper presented at the Proceedings of the 2nd international conference on Mobile systems, applications, and services, Boston, MA, USA, 177 - 189.

Hong, J. I., Ng, J. D., Lederer, S., & Landay, J. A. (2004). *Privacy risk models for designing privacy-sensitive ubiquitous computing systems.* Paper presented at the Proceedings of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques, Cambridge, MA, USA, 91 - 100.

Huda, M.N. (2007). *A Mobile Agent-based Privacy Protection Mechanism in Solving Multi-party Computation Problems*, Ph.D. thesis, The Graduate University for Advanced Studies.

Iachello, G., Smith, I., Consolvo, S., Abowd, G., Hughes, J., Howard, J., Potter, F., Scott, J., Sohn, T., Hightower, J., & LaMarca, A. (2005). *Control, Deception, and Communication:Evaluating the Deployment of a Location-Enhanced Messaging System.*.

Intel. (2004). *Placelab*. Retrieved 20/03/2005, available from: www.placelab.org.

lshaque, K. (2005). *Fundamental Rights in The Holy Qur'an*. Retrieved 24/03/2005, available from: http://quran.islamix.com/out.php?LinkID=94

Järvinen, P. (2000). *Research questions guiding selection of an appropriate research method*. In: Hansen, Bichler and Mahrer, Editors, Proceedings of ECIS2000, 3–5 July, Vienna University of Economics and Business Adminstration, Wien (2000), pp. 124–131.

Jiang, X., Hong, J. I., & Landay, J. A. (2002). *Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing.* Paper presented at the Fourth International Conference on Ubiquitous Computing, Goteberg, Sweden.

Johnson, A.P. (1995). *A Short Guide to Action Research.* Boston, Allyn & Bacon.

Jorns, O., & Bessler, S. (2004). *PRIVES: A privacy enhancing location based scheme.* Paper presented at the MobileHCI Workshop on Location Systems Privacy and Control, Glasgow, Scotland.

Junglas, I. A., & Spitzmueller, C. (2005). *A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services.* Paper presented at the 38th Hawaii International Conference on System Sciences, pp. 180b-180b.

Khalil, A., & Connelly, K. (2005). *Improving Cell Phone Awareness by Using Calendar Information.* In the Proceedings of International Conference on Human-Computer Interaction (INTERACT 2005), Rome, Italy, pp. 588-600.

Kjeldskov J., Skov M. B., Als B. S. and Høegh R. T. (2004). *Is it worth the hassle? Exploring the added value of evaluating the usability of context-aware mobile systems in the field.* In Proc. Mobile HCI 2004, 61--73.

Kjeldskov, J. and Graham, C. (2003). *A review of Mobile HCI Research Methods.* In Proceedings of Mobile HCI 2003, Springer-Verlag, LNCS 2795, 317-335.

Knight, K. (2003). *Lying*, Catholic Encyclopedia (Vol. ix).

Kotadia, M. (2004). *Nokia admits multiple Bluetooth security holes*. Retrieved 1/11/2004, available from: http://news.zdnet.co.uk/0,39020330,39145886,00.htm

Laasonen, K., Raento, M., Toivonen, H. (2004). *Adaptive On-Device Location Recognition*. In: Proc. Pervasive 2004 (2004) 287-304

Laitinen, H., Lahteenmaki, J., & Nordstrom, T. (2001). *Database correlation method for GSM location.* Paper presented at the 53rd IEEE Vehicular Technology Conference, Rhodes, Greece, May.

Langheinrich, M. (2001). *Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems.* Paper presented at the Proc. Ubicomp 2001, 273-291.

Langheinrich, M. (2002). *A Privacy Awareness System for Ubiquitous Computing Environments.* Paper presented at the 4th International Conference on Ubiquitous Computing (Ubicomp 2002), 237-245.

Lederer, S. (2003). *Designing Disclosure: Interactive Personal Privacy at the Dawn of Ubiquitous Computing*. available from: http://www.cs.berkeley.edu/projects/io/publications/privacy-lederer-msreport-1.01.pdf

Lederer, S., Dey, A. K., & Mankoff, J. (2002). *A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments* (Technical Report UCB/CSD-2-1188): Computer Science Division, University of California, Berkley. available from: http://www.cs.berkeley.edu/projects/io/publications/privacy-techreport02.pdf

Lederer, S., Hong, J. I., Dey, A. K., & Landay, J. A. (2004). *Personal privacy through understanding and action: five pitfalls for designers*. Personal and Ubiquitous Computing, 8(6), 440 - 454.

Lederer, S., Mankoff, J., & Dey, A. K. (2003). *Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing.* Paper presented at the Proceedings of Extended Abstracts of CHI 2003, ACM Conference on Human Factors in Computing Systems, Fort Lauderdale, FL, 724-725.

Lessig, L. (1998). *The Architecture of Privacy.* Paper presented at the Taiwan Net'98, Taipei, Taiwan.

Liao, L., Fox, D., Kautz, H.A. (2005). *Location-Based Activity Recognition using Relational Markov Networks.* In: Nineteenth International Joint Conference on Artificial Intelligence (IJCAI 2005), Edinburgh, Scotland.

McDougall, B. S. (2004). *Privacy*, New Encyclopedia of the History of Ideas (Vol. 5): Charles Scribner's Sons.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). *Values, personal information privacy, and regulatory approaches.* Communications of the ACM, *38*(12), 65-74.

Moore, B. (1984). *Privacy: Studies in Social and Cultural History*. Armonk, NY: New York: ME Sharpe.

Morson, G. S., & Emerson, C. (1991). *Mikhail Bakhtin: Creation of a Prosaics*: Stanford University Press.

Nguyen, D. H., & Mynatt, E. D. (2002). *Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems* (GIT-GVU-02-16): Georgia Institute of Technology. available from: http://quixotic.cc.gt.atl.ga.us/~dnguyen/research/PrivacyMirrors.pdf

Nielsen, J. (1994). *Heuristic evaluation*. In Nielsen, J., and Mack, R.L. (Eds.), Usability Inspection Methods, John Wiley & Sons, New York, NY.

Nielsen, J., and Molich, R. (1990). *Heuristic evaluation of user interfaces,* Proc. ACM CHI'90 Conf. (Seattle, WA, 1-5 April), 249-256.

Noam, E. (1997). *Privacy and Self-Regulation: Markets for Electronic Privacy*. available from: http://www.citi.columbia.edu/elinoam/articles/priv_self.htm

OECD. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available from: http://www1.oecd.org/publications/e-book/9302011E.PDF

OnlineDictionary. (2005). *Ubiquitous Computing*. Retrieved 03/05/05, 2005, available from: http://onlinedictionary.datasegment.com/word/ubiquitous+computing

Otsason, V., Varshavsky, A., LaMarca, A., & Lara, E. d. (2005). *Accurate GSM Indoor Localization.* Paper presented at the Ubicomp 2005, 141-158.

Oxford Dictionary of Law. ( 2002). *Deception*. In E. A. Martin (Ed.), A Dictionary of Law: Oxford University Press.

Palen, L. (1999). *Social, Individual & Technological Issues for Groupware Calendar Systems.* Paper presented at the ACM CHI '99 Conference.

Palen, L. & Dourish, P. (2003). *Unpacking "privacy" for a networked world*. Proceedings of the SIGCHI conference on Human factors in computing systems, April 05-10, 2003, Ft. Lauderdale, Florida, USA

Papakyriazis, N. V., & Boudourides, M. A. (2001). *Electronic Weak Ties in Network Organisations.* Paper presented at the 4th GOR Conference, Goettingen, Germany, May 17-18.

Pedersen, J. (2004). *Privacy and Location Technologies.* Paper presented at the Workshop on location systems privacy and control, MobileHCI'04, Glasgow, Scotland.

Plato. (360 B.C.E.). *Republic* (B. Jowett, Trans.).

Po, S., Howard, S., Vetere, F., & Skov, M. B. (2004). *Heuristic Evaluation and Mobile Usability: Bridging the Realism Gap*. In Mobile HCI, Glasgow UK.

Price, B. A., Adam, K., & Nuseibeh, B. (2005). *Keeping Ubiquitous Computing to Yourself: a practical model for user control of privacy*. International Journal of Human-Computer Studies, 63(1-2):228–253, July 2005.

Roussos, G. (2002). *Location Sensing Technologies and Applications*, TSW 02-08 November 2002, School of Computer Science and Information Systems Birkbeck College, University of London

SafeHabour. (2004). *Safe Habor Seal Program*, available from: http://www.export.gov/safeharbor/

Schon, D.A., (1983). *The reflective practitioner: How professionals think in action.* Basic Books, New York.

Singer, M. (2003). *Smart Dust Collecting in the Enterprise*. Retrieved 1/11/2004, available from: http://siliconvalley.internet.com/news/article.php/3098551

Smith, I., Consolvo, S., Lamarca, A., Hightower, J., James Scott, Sohn, T., Hughes, J., Iachello, G., & Abowd, G. D. (2005). *Social Disclosure of Place: From Location Technology to Communication Practices.* Paper presented at the 3rd Int'l Conf on Pervasive Computing: Pervasive '05, Munich, Germany.

Spinney, J. (2004). *Locations-Based Servives and the Proverbial Privacy Issue*. Retrieved 1/11/2004, available from: http://www.directionsmag.com/article.php?atricle id=510

Spitz, E. (1987). *Pointers for American Legislation on Computer Privacy: Insights from Jewish Law.* National Jewish Law Review II, 63-78.

Stone, D., Jarrett, C., Woodroffe, M., and Minocha, M. (2005). *User Interface Design And Evaluation*: Morgan Kaufmann.

Susman, G.I. and Evered, R.D. *An Assessment of the Scientific Merits of Action Research,* Administrative Science Quarterly, (23) 1978, pp. 582-603.

Taqiyah (2003). In J. L. Esposito (Ed.), *Oxford Dictionary of Islam*: Oxford University Press Inc.

TheFreeDictionary.com (2005). *Taqiya*. Retrieved 23/05/2005, available from: http://encyclopedia.thefreedictionary.com/Al-Taqiyya

Ustaran, E. (2003). *Data Protection And RFID Systems.* Privacy and Data Protection.

Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2003). *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems.* Paper presented at the First Intern.Conference on Security in Pervasive Computing (SPC).

Weiser, M., Gold, R., & Brown, J. S. (1999). *The origins of ubiquitous computing research at PARC in the late 1980s.* IBM Systems Journal, 38(4), 693-696.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

Wikipedia. (2005). *Privacy*, Retrieved on 7/11/2008, available from: http://en.wikipedia.org/wiki/Privacy

Worboys, M. F., & Clementini, E. (2001). *Integration of imperfect spatial information.* Journal of Visual Languages and Computing, 12, 61–80.

Worboys, M. F., & Duckham, M. (2004). *GIS: A Computing Perspective* (2nd edition ed.). Boca Raton, FL: CRC Press.

Wu, X., Liu, J., Hong, X., and Bertino, E. (2008). *Anonymous Geo-Forwarding in MANETs through Location Cloaking*. IEEE Trans. Parallel Distrib. Syst. 19, 10 (Oct. 2008), 1297-1309. DOI= http://dx.doi.org/10.1109/TPDS.2008.28

Yamada, S., & Kamioka, E. (2005). *Access Control for Security and Privacy in Ubiquitous Computing Environments.* IEICE Transactions on Communications, E88-B(3), 846-856.

ZDNET (2008). *Mobile Computing.* Retrieved on 7/11/2008, available from http://dictionary.zdnet.com/definition/mobile+computing.html

# Appendix A

This section illustrates a description of the online scenario-based study outlined in Chapter 3. The study was administered using the Open University's ELSA (**https://elsa.open.ac.uk**) system.

**STUDY ON LOCATION DISCLOSURE**

We are conducting research into the use of various techniques to control privacy as it relates to your mobile phone. In particular we are interested in how people can control the disclosure of their location and the ways in which they might need to provide false or imprecise information. The aim of this work is to ensure that the technology empowers people instead of removing their privacy. We would be grateful if you completed this questionnaire to aid in our research. It should take between 5 and 10 minutes to complete and all answers will remain strictly confidential.

**BACKGROUND**

As you may be aware, if you carry an ordinary mobile telephone it is possible for your mobile telephone network to track your location with an accuracy of between 100 m and 1000 m within most urban areas, although this accuracy is set to increase soon. You may also subscribe to services which will let others see your location. You might be able to imagine some of the benefits of this kind of service, such as:

1. Safety - families, friends and loved ones are able to keep track of each other (especially keeping track of kids while they are away from their parents) or you can be located in case of an emergency.
2. Location Based Services – getting directions to the nearest bank machine, tourist information about the site you are standing in front of, and so on.
3. Improved efficiency - businesses (e.g. Taxi services, sales reps) use location-tracking systems to find out who is closer to a client.

Possible limitations in the use of these systems are:

1. Loss of privacy, feeling of being constantly under surveillance.
2. Profiling as a result of inference of activity from one's location, location based spam (getting text messages from a shop as you pass it).
3. Lack of control of what location to disclose to whom and at what time (in most cases only consent is sought from the data subject).

Imagine you and people in your social network have a location-tracking system (on your mobile phones) which may permit you to keep track of each other's location. People within your social network will typically include (but not limited to) friends, spouse/partner, colleagues, boss, and family. Imagine you are able to manipulate and control what location to reveal to whom, and at what time. Further imagine that you are able to disclose a location different from your true location using a privacy control feature that comes with the location tracking service. This gives you the ability not only to send an untrue location, but also to make the disclosed location look plausible enough for the requestor. In the following questions, please assume that your mobile phone is capable of handling all the above functions.

begin questionnaire>>

**General Disclosure**

**In general, and in circumstances where it would in no way be embarrassing to reveal your location to the person, how do you think you would disclose your location/activity to the following people?**

**Note: Your responses will only be recorded or saved once you click the submit button. Therefore you can choose to opt out of the study at anytime.**

| | |
|---|---|
| **spouse/partner** | ○ **always provide exact location** |
| | ○ **give false location information** |
| | ○ **vary the precision of location information** |
| | ○ **ignore request** |

| | |
|---|---|
| | ☐ Other (please specify) |
| Colleague | ☐ always provide exact location<br>☐ give false location information<br>☐ vary the precision of location information<br>☐ ignore request<br>☐ Other (please specify) |
| Boss | ☐ always provide exact location<br>☐ give false location information<br>☐ vary the precision of location information<br>☐ ignore request<br>☐ Other (please specify) |
| Parent (i.e. if you are under 18) | ☐ always provide exact location<br>☐ give false location information<br>☐ vary the precision of location information<br>☐ ignore request<br>☐ Other (please specify) |
| Friend | ☐ always provide exact location<br>☐ give false location information<br>☐ vary the precision of location information<br>☐ ignore request<br>☐ Other (please specify) |
| Child | ☐ always provide exact location<br>☐ give false location information |

| | |
|---|---|
| | ☐ vary the precision of location information<br>☐ ignore request<br>☐ Other (please specify)<br>[ ] |
| Another member of the family | ☐ always provide exact location<br>☐ give false location information<br>☐ vary the precision of location information<br>☐ ignore request<br>☐ Other (please specify)<br>[ ] |
| Stranger | ☐ always provide exact location<br>☐ give false location information<br>☐ vary the precision of location information<br>☐ ignore request<br>☐ Other (please specify)<br>[ ] |

<< previous page | next page >>

**The use of deception in social mobile computing**

**For each of the questions below, we want you to imagine yourself in that circumstance in which you are asked to disclose your location, but might not wish to do so. For each person who might ask you in this type of situation, please score how likely you would be to provide false information using your mobile phone, and how comfortable you would be deceiving this person in this situation.**

**SECTION A: Disclosing an untrue location with good intention**

- **For instance, you are in a gift shop about to buy a surprise gift for a person. You set your phone to reveal a different but plausible location to that person when they ask for your location.**

| | Very likely | 2 | 3 | 4 | Not at all Likely |
|---|---|---|---|---|---|
| How likely would you be to engage in this deception if the person was your *spouse/partner*? | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| **How <u>comfortable</u> would you feel deceiving your *spouse/partner* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>likely</u> would you be to engage in this deception if the person was your *boss*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>comfortable</u> would you feel deceiving your *boss* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Please answer this (and the next) only if you are under 18 years of age.<br><br>How <u>likely</u> would you be to engage in this deception if the person was your *parent*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>comfortable</u> would you feel deceiving your *parent* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>likely</u> would you be to engage in this deception if the person was your *work colleague*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>comfortable</u> would you feel deceiving your *work colleague* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>likely</u> would you be to engage in this deception if the person was your *friend*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>comfortable</u> would you feel deceiving your *friend* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>likely</u> would you be to engage in this deception if the person was your *child*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| **How comfortable would you feel deceiving your *child* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How likely would you be to engage in this deception if the person was another *member of your family*** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How comfortable would you feel deceiving another *member of your family* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |

**Please use the space below to provide any comments you may have regarding the above responses, if any.**

<< previous page | next page >>

---

**SECTION B: Disclosing an untrue location to maintain social harmony**

**For Example,**

**The person wants to know your location/activity while you are engaged in an activity you do not want him/her to know.**

**You are running late to meet the person.You do not want him/her to know you have still not left.**

**You have very little time to complete a task and you don't want the person to know you are nearby as social convention would require you to talk to him/her.**

| | | | | | |
|---|---|---|---|---|---|
| **How likely would you be to engage in this deception if the person was your *spouse/partner?*** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How comfortable would you feel deceiving your *spouse/partner* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How likely would you be to engage in this deception if the person was your *boss*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |

| | | | | | |
|---|---|---|---|---|---|
| |  |  |  |  |  |
| How comfortable would you feel deceiving your *boss* in this circumstance? | Very Comfortable | 2 | 3 | 4 | Not at all Comfortable |
| |  |  |  |  |  |
| Please answer this (and the next) only if you are under 18 years of age.<br><br>How likely would you be to engage in this deception if the person was your *parent*? | Very likely | 2 | 3 | 4 | Not at all Likely |
| |  |  |  |  |  |
| How comfortable would you be to engage in this deception if the person was your *parent*? | Very comfortable | 2 | 3 | 4 | Not at all comfortable |
| |  |  |  |  |  |
| How likely would you be to engage in this deception if the person was your *work colleague*? | Very likely | 2 | 3 | 4 | Not at all Likely |
| |  |  |  |  |  |
| How comfortable would you feel deceiving your *work colleague* in this circumstance? | Very Comfortable | 2 | 3 | 4 | Not at all Comfortable |
| |  |  |  |  |  |
| How likely would you be to engage in this deception if the person was your *friend*? | Very likely | 2 | 3 | 4 | Not at all Likely |
| |  |  |  |  |  |
| How comfortable would you feel deceiving your *friend* in this circumstance? | Very Comfortable | 2 | 3 | 4 | Not at all Comfortable |
| |  |  |  |  |  |
| How likely would you be to engage in this deception if the person was your *child*? | Very likely | 2 | 3 | 4 | Not at all Likely |
| |  |  |  |  |  |
| How comfortable would you feel deceiving your *child* in this circumstance? | Very Comfortable | 2 | 3 | 4 | Not at all Comfortable |
| |  |  |  |  |  |
| How likely would you be to engage in this deception if the person was *another* | Very likely | 2 | 3 | 4 | Not at all Likely |

| | | | | | |
|---|---|---|---|---|---|
| *member of your family* | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How comfortable would you feel deceiving *another member of your family* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |

**Please use the space below to provide any comments you may have regarding the above responses, if any.**

**Please use the space below to provide any comments you may have regarding the above responses, if any.**

<< previous page  next page >>

---

**SECTION C: Disclosing an untrue location in situations which can neither be classified as being of good intention or maintaining social harmony.**

**For example, you are in a location or engaged in an activity you will feel embarrassed for the requestor to know.**

| | | | | | |
|---|---|---|---|---|---|
| **How likely would you be to engage in this deception if the person was your *spouse/partner?*** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How comfortable would you feel deceiving your *spouse/partner* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How likely would you be to engage in this deception if the person was your *boss*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | |
|---|---|---|---|---|---|
| **How <u>comfortable</u> would you feel deceiving your *boss*?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Please answer this (and the next) only if you are under 18 years of age.**<br><br>**How <u>likely</u> would you be to engage in this deception if the person was your *parent*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>comfortable</u> would you feel deceiving your *parent*?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>likely</u> would you be to engage in this deception if the person was your *work colleague*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>comfortable</u> would you feel deceiving your *work colleague* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>likely</u> would you be to engage in this deception if the person was your *friend*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>comfortable</u> would you feel deceiving your *friend* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>likely</u> would you be to engage in this deception if the person was your *child*?** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>comfortable</u> would you feel deceiving your *child* in this circumstance?** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>likely</u> would you be to engage in this deception if the person was *another member of your family?*** | **Very likely** | **2** | **3** | **4** | **Not at all Likely** |
| | ☐ | ☐ | ☐ | ☐ | ☐ |
| **How <u>comfortable</u> would you feel deceiving *another member of your family*** | **Very Comfortable** | **2** | **3** | **4** | **Not at all Comfortable** |

| in this circumstance? | | | | | |
|---|---|---|---|---|---|

**Please use the space below to provide any comments you may have regarding the above responses, if any.**

<< previous page  next page >>

---

**PLAUSIBLE LOCATION DISCLOSURE**

Disclosing one's location, whether a true disclosure or not, requires that the disclosed location makes sense to the requestor. For instance, if the requestor is in a different country or even in a different continent, a fine-grained disclosure may not be necessary. To illustrate this, responding to a location request from a requestor (in another country or continent) with the answer: "I'm at KMI podium" may not make much sense to the requestor if he/she does not know what or where KMI podium is. Responding with say, "I'm in Milton Keynes" may be more appropriate in this case. This may or may not require knowing some information about the requestor in order to disclose a location that is plausible enough, depending on who is disclosing the location.

Based on the above, what information about the requestor will you want to know before disclosing your location (assuming it is possible to know such information on your mobile phone)? Please choose one.

- the approximate location of the requestor at the time of the request
- the reason for the request
- I do not wish to know any information
- Other (please specify)

<< previous page  submit >>

---

# Appendix B

This section describes in detail the between-subjects study described in Section 3.7.

### Mobile phones and location-disclosure study

Thank you for responding to our request for help with our survey. This study is hosted by Karim Adam, a PhD student at the Open University Computing Research Centre.

As you may be aware, if you carry an ordinary mobile telephone it is possible for your mobile telephone network to track your location with an accuracy of between 100 m and 1000 m within most urban areas, although this accuracy is set to increase soon. You may also subscribe to services which will let others see your location. You might be able to imagine some of the benefits of this kind of service, such as:

- Safety - families, friends and loved ones are able to keep track of each other (especially keeping track of kids while they are away from their parents) or you can be located in case of an emergency.
- Location Based Services - getting directions to the nearest bank machine, tourist information about the site you are standing in front of, and so on.
- Improved efficiency - businesses (e.g. Taxi services, sales reps) use location-tracking systems to find out who is closer to a client.

Possible limitations in the use of these systems are:

- Loss of privacy, feeling of being constantly under surveillance.
- Profiling as a result of inference of activity from one's location, location-based spam (getting text messages from a shop as you pass it).
- Lack of control of what location to disclose to whom and at what time.

On the following page, we are going to present you with a scenario that would involve not disclosing your location to another via a mobile phone. We want you to imagine how you would feel and react in such a situation, even if you don't own a mobile phone, or wouldn't normally act in the way shown in the scenario.

If you are happy to continue please select 'Click here to begin the study' below:'

Click here to begin the study

Mobile Phone Location

Please imagine that you are in a gift shop about to buy a surprise gift for a friend. As you are in the shop, your phone beeps. It is your friend, the intended recipient of the gift, asking where you are. You click on the '**do not disclose true location**' response, which tells your friend that you are in a completely different location - at work. There is a **high possibility** that your friend will discover that you have not been entirely honest disclosing your location.

Imagining that you were in this scenario, please answer the questions below:

**1. How comfortable would you be giving this response to their location query?**

Very much ○ ○ ○ ○ ○ Not at all

**2. Would you see your response as a form of deception?**

Very much ○ ○ ○ ○ ○ Not at all

**3. How likely do you think that your response might be discovered by your friend?**

Very much ○ ○ ○ ○ ○ Not at all

**4. Would you have an ethical problem engaging in this type of response?**

Very much ○ ○ ○ ○ ○ Not at all

**5. If you were faced with this scenario in real life, how likely is it that you would respond in the same way as in the scenario?**

Very much ○ ○ ○ ○ ○ Not at all

**6. If you would like to make any further comments, please type them here:**

**7. Finally, could you please tell us:**

**Your age** _____ **(years)**

**Your gender:** _____

**Thank you for taking the time to complete this questionnaire,**
**your help is very important to us.**

**If you are happy with your responses, please click the submit button below.**

Submit

**If you have any difficulty using this questionnaire, please e-mail the OU's internet survey staff.**

Mobile Phone Location

Please imagine that you are in a gift shop about to buy a surprise gift for a friend. As you are in the shop, your phone beeps. It is your friend, the intended recipient of the gift, asking where you are. You click on the **'be ambiguous'** response, which only tells your friend that you are in the town centre, not in the specific gift shop. There is a **high possibility** that your friend will discover that you have not been entirely honest disclosing your location.

Imagining that you were in this scenario, please answer the questions below:

**1. How comfortable would you be giving this response to their location query?**

Very much Not at all

**2. Would you see your response as a form of deception?**

Very much Not at all

**3. How likely do you think that your response might be discovered by your friend?**

Very much Not at all

**4. Would you have an ethical problem engaging in this type of response?**

Very much Not at all

**5. If you were faced with this scenario in real life, how likely is it that you would respond in the same way as in the scenario?**

Very much Not at all

**6. If you would like to make any further comments, please type them here:**

**7. Finally, could you please tell us:**

**Your age** (years)

**Your gender:**

**Thank you for taking the time to complete this questionnaire,**
**your help is very important to us.**

**If you are happy with your responses, please click the submit button below.**

Submit

**If you have any difficulty using this questionnaire, please e-mail the OU's internet survey staff.**

Mobile Phone Location

Please imagine that you are in a gift shop about to buy a surprise gift for a friend. As you are in the shop, your phone beeps. It is your friend, the intended recipient of the gift, asking where you are. You click on the '**be ambiguous**' response, which only tells your friend that you are in the town centre, not in the specific gift shop. There is **very little possibility** that your friend will discover that you have not been entirely honest disclosing your location.

Imagining that you were in this scenario, please answer the questions below:

**1. How comfortable would you be giving this response to their location query?**

Very much Not at all

2. **Would you see your response as a form of deception?**

Very much Not at all

3. **How likely do you think that your response might be discovered by your friend?**

Very much Not at all

4. **Would you have an ethical problem engaging in this type of response?**

Very much Not at all

5. **If you were faced with this scenario in real life, how likely is it that you would respond in the same way as in the scenario?**

Very much Not at all

**6. If you would like to make any further comments, please type them here:**

**7. Finally, could you please tell us:**

**Your age** (years)

**Your gender:**

**Thank you for taking the time to complete this questionnaire,**
**your help is very important to us.**

**If you are happy with your responses, please click the submit button below.**

Submit

**If you have any difficulty using this questionnaire, please e-mail the OU's internet survey staff.**

Mobile Phone Location

Please imagine that you are in a gift shop about to buy a surprise gift for a friend. As you are in the shop, your phone beeps. It is your friend, the intended recipient of the gift, asking where you are. You click on the '**do not disclose true location**' response, which tells your friend that you are in a completely different location - at work. There is **very little possibility** that your friend will discover that you have not been entirely honest disclosing your location.

Imagining that you were in this scenario, please answer the questions below:

**1. How comfortable would you be giving this response to their location query?**

Very much ○ ○ ○ ○ ○ Not at all

**2. Would you see your response as a form of deception?**

Very much ○ ○ ○ ○ ○ Not at all

**3. How likely do you think that your response might be discovered by your friend?**

Very much ○ ○ ○ ○ ○ Not at all

**4. Would you have an ethical problem engaging in this type of response?**

Very much ○ ○ ○ ○ ○ Not at all

**5. If you were faced with this scenario in real life, how likely is it that you would respond in the same way as in the scenario?**

Very much ○ ○ ○ ○ ○ Not at all

**6. If you would like to make any further comments, please type them here:**

**7. Finally, could you please tell us:**

**Your age** ____ **(years)**

**Your gender:** ____

**Thank you for taking the time to complete this questionnaire,**
**your help is very important to us.**

**If you are happy with your responses, please click the submit button below.**

Submit

**If you have any difficulty using this questionnaire, please e-mail the OU's internet survey staff.**

# Appendix C

This is processed data captured from the between-the-subject study in Appendix B using the statistical tool SPSS.

**Chi Square Test Results**

| Possibility of discovery versus level of discomfort crosstabulation | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | Total |
| Possibility of discovery | High possibility of discovery | 64 | 60 | 37 | 60 | 46 | 267 |
| | Low possibility of discovery | 85 | 58 | 36 | 28 | 29 | 236 |
| Total | | 149 | 118 | 73 | 88 | 75 | 503 |

| Chi-Square Tests for possibility of discovery versus level of discomfort crosstabulation | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 16.650[a] | 4 | .002 |
| Likelihood Ratio | 16.900 | 4 | .002 |
| Linear-by-Linear Association | 13.192 | 1 | .000 |
| N of Valid Cases | 503 | | |
| a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 34.25. | | | |

| Technique used to protect privacy versus level of discomfort Crosstabulation | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | Total |
| Techninque used to protect privacy | Deception | 65 | 52 | 38 | 53 | 55 | 263 |
| | Blurring | 84 | 66 | 35 | 35 | 20 | 240 |
| Total | | 149 | 118 | 73 | 88 | 75 | 503 |

| Chi-Square Tests for technique used to protect privacy versus level of discomfort crosstabulation | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 23.219[a] | 4 | .000 |
| Likelihood Ratio | 23.858 | 4 | .000 |
| Linear-by-Linear Association | 21.123 | 1 | .000 |
| N of Valid Cases | 503 | | |
| a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 34.83. | | | |

| Level of ethics concern versus technique used to protect privacy | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | Total |
| Technique used to protect privacy | Deception | 54 | 58 | 36 | 38 | 77 | 263 |
| | Blurring | 15 | 37 | 25 | 46 | 114 | 237 |
| Total | | 69 | 95 | 61 | 84 | 191 | 500 |

| Level of ethics concern versus technique used to protect privacy | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 35.342[a] | 4 | .000 |
| Likelihood Ratio | 36.698 | 4 | .000 |
| Linear-by-Linear Association | 33.609 | 1 | .000 |
| N of Valid Cases | 500 | | |
| a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 28.91. | | | |

| Level of ethics concern versus possibility of discovery crosstab | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | |
| Possibility of discovery | High possibility of discovery | 38 | 57 | 29 | 41 | 100 | 265 |
| | Low possibility of discovery | 31 | 38 | 32 | 43 | 91 | 235 |
| Total | | 69 | 95 | 61 | 84 | 191 | 500 |

| Chi-Square Tests for Level of ethics concern versus possibility of discovery crosstab | | | |
|---|---|---|---|
| | Value | df | Asymp. Sig. (2-sided) |
| Pearson Chi-Square | 3.341[a] | 4 | .502 |
| Likelihood Ratio | 3.355 | 4 | .500 |
| Linear-by-Linear Association | .866 | 1 | .352 |
| N of Valid Cases | 500 | | |
| a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 28.67. | | | |

**Univariate Analysis of Variance**

**Between-Subjects Factors**

| | | Value Label | N |
|---|---|---|---|
| Possibility of discovery | 1.00 | High possibility of discovery | 267 |
| | 2.00 | Low possibility of discovery | 236 |
| Techninque used to protect privacy | 1.00 | Deception | 263 |
| | 2.00 | Blurring | 240 |

**Descriptive Statistics**

Dependent Variable: q1

| Possibility of discovery | Techninque used | Mean | Std. Deviation | N |
|---|---|---|---|---|
| High possibility of discovery | Deception | 3.19 | 1.488 | 137 |
| | Blurring | 2.52 | 1.319 | 130 |
| | Total | 2.87 | 1.445 | 267 |
| Low possibility of discovery | Deception | 2.64 | 1.450 | 126 |
| | Blurring | 2.12 | 1.276 | 110 |
| | Total | 2.40 | 1.394 | 236 |
| Total | Deception | 2.93 | 1.493 | 263 |
| | Blurring | 2.34 | 1.312 | 240 |
| | Total | 2.65 | 1.439 | 503 |

**Estimated Marginal Means**

**1. Possibility of discovery**

Dependent Variable: q1

| Possibility of discovery | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| High possibility of discovery | 2.856 | .085 | 2.689 | 3.024 |
| Low possibility of discovery | 2.381 | .091 | 2.202 | 2.559 |

**2. Techninque used to protect privacy**

Dependent Variable: q1

| Techninque used to protect privacy | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| Deception | 2.916 | .086 | 2.748 | 3.085 |
| Blurring | 2.321 | .090 | 2.144 | 2.498 |

**3. Possibility of discovery * Techninque used to protect privacy**

Dependent Variable: q1

| Possibility of discovery | Techninque used to protect privacy | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|---|
| | | | | Lower Bound | Upper Bound |
| High possibility of discovery | Deception | 3.190 | .119 | 2.956 | 3.423 |
| | Blurring | 2.523 | .122 | 2.283 | 2.763 |
| Low possibility of discovery | Deception | 2.643 | .124 | 2.399 | 2.886 |
| | Blurring | 2.118 | .133 | 1.858 | 2.379 |

**Univariate Analysis of Variance**

**Between-Subjects Factors**

| | | Value Label | N |
|---|---|---|---|
| Possibility of discovery | 1.00 | High possibility of discovery | 267 |
| | 2.00 | Low possibility of discovery | 236 |
| Techninque used to protect privacy | 1.00 | Deception | 263 |
| | 2.00 | Blurring | 240 |

**Descriptive Statistics**

Dependent Variable: q2

| Possibility of discovery | Techninque used | Mean | Std. Deviation | N |
|---|---|---|---|---|
| High possibility of discovery | Deception | 2.32 | 1.339 | 137 |
| | Blurring | 3.70 | 1.316 | 130 |
| | Total | 2.99 | 1.494 | 267 |
| Low possibility of discovery | Deception | 2.65 | 1.450 | 126 |
| | Blurring | 3.80 | 1.333 | 110 |
| | Total | 3.19 | 1.507 | 236 |
| Total | Deception | 2.48 | 1.400 | 263 |
| | Blurring | 3.75 | 1.322 | 240 |
| | Total | 3.08 | 1.502 | 503 |

**Tests of Between-Subjects Effects**

Dependent Variable: q2

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Corrected Model | 209.090[a] | 3 | 69.697 | 37.663 | .000 |
| Intercept | 4858.048 | 1 | 4858.048 | 2625.251 | .000 |
| discover | 5.765 | 1 | 5.765 | 3.115 | .078 |
| techniqu | 199.600 | 1 | 199.600 | 107.862 | .000 |
| discover * techniqu | 1.647 | 1 | 1.647 | .890 | .346 |
| Error | 923.404 | 499 | 1.851 | | |
| Total | 5915.000 | 503 | | | |
| Corrected Total | 1132.493 | 502 | | | |

a. R Squared = .185 (Adjusted R Squared = .180)

**Estimated Marginal Means**

**1. Possibility of discovery**

Dependent Variable: q2

| Possibility of discovery | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| High possibility of discovery | 3.011 | .083 | 2.847 | 3.174 |
| Low possibility of discovery | 3.225 | .089 | 3.051 | 3.400 |

**2. Techninque used to protect privacy**

Dependent Variable: q2

| Techninque used to protect privacy | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| Deception | 2.486 | .084 | 2.321 | 2.651 |
| Blurring | 3.750 | .088 | 3.577 | 3.923 |

**3. Possibility of discovery * Techninque used to protect privacy**

Dependent Variable: q2

| Possibility of discovery | Techninque used to protect privacy | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|---|
| | | | | Lower Bound | Upper Bound |
| High possibility of discovery | Deception | 2.321 | .116 | 2.093 | 2.550 |
| | Blurring | 3.700 | .119 | 3.466 | 3.934 |
| Low possibility of discovery | Deception | 2.651 | .121 | 2.413 | 2.889 |
| | Blurring | 3.800 | .130 | 3.545 | 4.055 |

**Univariate Analysis of Variance**

**Between-Subjects Factors**

| | | Value Label | N |
|---|---|---|---|
| Possibility of discovery | 1.00 | High possibility of discovery | 266 |
| | 2.00 | Low possibility of discovery | 235 |
| Techninque used to protect privacy | 1.00 | Deception | 262 |
| | 2.00 | Blurring | 239 |

**Descriptive Statistics**

Dependent Variable: q3

| Possibility of discovery | Techninque used | Mean | Std. Deviation | N |
|---|---|---|---|---|
| High possibility of discovery | Deception | 2.83 | 1.119 | 136 |
| | Blurring | 2.73 | 1.048 | 130 |
| | Total | 2.78 | 1.084 | 266 |
| Low possibility of discovery | Deception | 3.38 | 1.080 | 126 |
| | Blurring | 3.48 | 1.077 | 109 |
| | Total | 3.43 | 1.077 | 235 |
| Total | Deception | 3.10 | 1.132 | 262 |
| | Blurring | 3.07 | 1.122 | 239 |
| | Total | 3.08 | 1.126 | 501 |

**Tests of Between-Subjects Effects**

Dependent Variable: q3

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Corrected Model | 52.885[a] | 3 | 17.628 | 15.064 | .000 |
| Intercept | 4796.860 | 1 | 4796.860 | 4099.146 | .000 |
| discover | 52.263 | 1 | 52.263 | 44.661 | .000 |
| techniqu | .000 | 1 | .000 | .000 | .984 |
| discover * techniqu | 1.197 | 1 | 1.197 | 1.023 | .312 |
| Error | 581.594 | 497 | 1.170 | | |
| Total | 5399.000 | 501 | | | |
| Corrected Total | 634.479 | 500 | | | |

a. R Squared = .083 (Adjusted R Squared = .078)

**Estimated Marginal Means**

**1. Possibility of discovery**

Dependent Variable: q3

| Possibility of discovery | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| High possibility of discovery | 2.781 | .066 | 2.650 | 2.911 |
| Low possibility of discovery | 3.429 | .071 | 3.290 | 3.568 |

**2. Techninque used to protect privacy**

Dependent Variable: q3

| Techninque used to protect privacy | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| Deception | 3.106 | .067 | 2.975 | 3.237 |
| Blurring | 3.104 | .070 | 2.966 | 3.242 |

**3. Possibility of discovery * Techninque used to protect privacy**

Dependent Variable: q3

| Possibility of discovery | Techninque used to protect privacy | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|---|
| | | | | Lower Bound | Upper Bound |
| High possibility of discovery | Deception | 2.831 | .093 | 2.649 | 3.013 |
| | Blurring | 2.731 | .095 | 2.544 | 2.917 |
| Low possibility of discovery | Deception | 3.381 | .096 | 3.192 | 3.570 |
| | Blurring | 3.477 | .104 | 3.273 | 3.681 |

## Univariate Analysis of Variance

**Between-Subjects Factors**

| | | Value Label | N |
|---|---|---|---|
| Techninque used to protect privacy | 1.00 | Deception | 263 |
| | 2.00 | Blurring | 237 |
| Possibility of discovery | 1.00 | High possibility of discovery | 265 |
| | 2.00 | Low possibility of discovery | 235 |

**Descriptive Statistics**

Dependent Variable: q4

| Techninque used | Possibility of discovery | Mean | Std. Deviation | N |
|---|---|---|---|---|
| Deception | High possibility of discovery | 2.97 | 1.557 | 137 |
| | Low possibility of discovery | 3.24 | 1.504 | 126 |
| | Total | 3.10 | 1.535 | 263 |
| Blurring | High possibility of discovery | 3.88 | 1.322 | 128 |
| | Low possibility of discovery | 3.87 | 1.348 | 109 |
| | Total | 3.87 | 1.331 | 237 |
| Total | High possibility of discovery | 3.41 | 1.515 | 265 |
| | Low possibility of discovery | 3.53 | 1.465 | 235 |
| | Total | 3.47 | 1.492 | 500 |

**Tests of Between-Subjects Effects**

Dependent Variable: q4

| Source | | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Intercept | Hypothesis | 6044.046 | 1 | 6044.046 | 82.498 | .071 |
| | Error | 72.902 | .995 | 73.263[a] | | |
| techniqu | Hypothesis | 73.377 | 1 | 73.377 | 32.258 | .111 |
| | Error | 2.275 | 1 | 2.275[b] | | |
| discover | Hypothesis | 2.161 | 1 | 2.161 | .950 | .508 |
| | Error | 2.275 | 1 | 2.275[b] | | |
| techniqu * discover | Hypothesis | 2.275 | 1 | 2.275 | 1.094 | .296 |
| | Error | 1030.942 | 496 | 2.079[c] | | |

a. MS(techniqu) + MS(discover) - MS(techniqu * discover)

b. MS(techniqu * discover)

c. MS(Error)

**Expected Mean Squares[a,b]**

| Source | Variance Component | | | | |
|---|---|---|---|---|---|
| | Var(techniqu) | Var(discover) | Var(techniqu * discover) | Var(Error) | Quadratic Term |
| Intercept | 248.273 | 248.273 | 124.137 | 1.000 | Intercept |
| techniqu | 248.273 | .000 | 124.137 | 1.000 | |
| discover | .000 | 248.273 | 124.137 | 1.000 | |
| techniqu * discover | .000 | .000 | 124.137 | 1.000 | |
| Error | .000 | .000 | .000 | 1.000 | |

a. For each source, the expected mean square equals the sum of the coefficients in the cells times the variance components, plus a quadratic term involving effects in the Quadratic Term cell.

b. Expected Mean Squares are based on the Type III Sums of Squares.

## Estimated Marginal Means

**1. Techninque used to protect privacy * Possibility of discovery**

Dependent Variable: q4

| Techninque used to protect privacy | Possibility of discovery | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|---|
| | | | | Lower Bound | Upper Bound |
| Deception | High possibility of discovery | 2.971 | .123 | 2.729 | 3.213 |
| | Low possibility of discovery | 3.238 | .128 | 2.986 | 3.490 |
| Blurring | High possibility of discovery | 3.875 | .127 | 3.625 | 4.125 |
| | Low possibility of discovery | 3.872 | .138 | 3.600 | 4.143 |

**2. Possibility of discovery**

Dependent Variable: q4

| Possibility of discovery | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| High possibility of discovery | 3.423 | .089 | 3.249 | 3.597 |
| Low possibility of discovery | 3.555 | .094 | 3.370 | 3.740 |

**3. Techninque used to protect privacy**

Dependent Variable: q4

| Techninque used to protect privacy | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| Deception | 3.104 | .089 | 2.930 | 3.279 |
| Blurring | 3.873 | .094 | 3.689 | 4.058 |

## Univariate Analysis of Variance

**Between-Subjects Factors**

| | | Value Label | N |
|---|---|---|---|
| Techninque used to protect privacy | 1.00 | Deception | 261 |
| | 2.00 | Blurring | 239 |
| Possibility of discovery | 1.00 | High possibility of discovery | 266 |
| | 2.00 | Low possibility of discovery | 234 |

**Descriptive Statistics**

Dependent Variable: q5

| Techninque used | Possibility of discovery | Mean | Std. Deviation | N |
|---|---|---|---|---|
| Deception | High possibility of discovery | 2.90 | 1.541 | 136 |
| | Low possibility of discovery | 2.74 | 1.577 | 125 |
| | Total | 2.82 | 1.557 | 261 |
| Blurring | High possibility of discovery | 2.28 | 1.353 | 130 |
| | Low possibility of discovery | 1.91 | 1.259 | 109 |
| | Total | 2.11 | 1.321 | 239 |
| Total | High possibility of discovery | 2.59 | 1.482 | 266 |
| | Low possibility of discovery | 2.35 | 1.493 | 234 |
| | Total | 2.48 | 1.491 | 500 |

**Tests of Between-Subjects Effects**

Dependent Variable: q5

| Source | | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Intercept | Hypothesis | 2991.903 | 1 | 2991.903 | 41.304 | .069 |
| | Error | 88.162 | 1.217 | 72.436[a] | | |
| techniqu | Hypothesis | 65.065 | 1 | 65.065 | 48.638 | .091 |
| | Error | 1.338 | 1 | 1.338[b] | | |
| discover | Hypothesis | 8.709 | 1 | 8.709 | 6.511 | .238 |
| | Error | 1.338 | 1 | 1.338[b] | | |
| techniqu * discover | Hypothesis | 1.338 | 1 | 1.338 | .640 | .424 |
| | Error | 1035.960 | 496 | 2.089[c] | | |

a. MS(techniqu) + MS(discover) - MS(techniqu * discover)

b. MS(techniqu * discover)

c. MS(Error)

**Expected Mean Squares[a,b]**

| Source | Variance Component | | | | |
|---|---|---|---|---|---|
| | Var(techniqu) | Var(discover) | Var(techniqu * discover) | Var(Error) | Quadratic Term |
| Intercept | 248.296 | 248.296 | 124.148 | 1.000 | Intercept |
| techniqu | 248.296 | .000 | 124.148 | 1.000 | |
| discover | .000 | 248.296 | 124.148 | 1.000 | |
| techniqu * discover | .000 | .000 | 124.148 | 1.000 | |
| Error | .000 | .000 | .000 | 1.000 | |

a. For each source, the expected mean square equals the sum of the coefficients in the cells times the variance components, plus a quadratic term involving effects in the Quadratic Term cell.

b. Expected Mean Squares are based on the Type III Sums of Squares.

## Estimated Marginal Means

### 1. Techninque used to protect privacy * Possibility of discovery

Dependent Variable: q5

| Techninque used to protect privacy | Possibility of discovery | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|---|
| | | | | Lower Bound | Upper Bound |
| Deception | High possibility of discovery | 2.897 | .124 | 2.654 | 3.141 |
| | Low possibility of discovery | 2.736 | .129 | 2.482 | 2.990 |
| Blurring | High possibility of discovery | 2.277 | .127 | 2.028 | 2.526 |
| | Low possibility of discovery | 1.908 | .138 | 1.636 | 2.180 |

### 2. Possibility of discovery

Dependent Variable: q5

| Possibility of discovery | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| High possibility of discovery | 2.587 | .089 | 2.413 | 2.761 |
| Low possibility of discovery | 2.322 | .095 | 2.136 | 2.508 |

### 3. Techninque used to protect privacy

Dependent Variable: q5

| Techninque used to protect privacy | Mean | Std. Error | 95% Confidence Interval | |
|---|---|---|---|---|
| | | | Lower Bound | Upper Bound |
| Deception | 2.817 | .090 | 2.641 | 2.992 |
| Blurring | 2.093 | .094 | 1.908 | 2.277 |

# Appendix D: Post User Study Responses

This section provides data captured in the post user study. They are responses provided by participants after every request/disclosure was made during the entire duration of the study.

| Participant | Date | Objective of Disclosure | Post-disclosure question | Response |
|---|---|---|---|---|
| **Requestor 1** | 21/05/2007 | True Location | How true was the response from Mark when he said he was at home today at 8am? | True |
| | 21/05/2007 | False Location | How true was the response from Adam when he said he was at the City Centre today at 8:05am? | Very true |
| | 22/05/2007 | False Location plus Activity | How true was the response from Adam when he said he was at home watching TV today at 8:15am? | Fairly true |
| | 22/05/2007 | Blurred Location | How true was the response from Mark when he said he was at the City Centre today at 11am? | Very true |
| | 23/05/2007 | True Location plus Activity | How true was the response from Mark when he said he was at Tesco doing some shopping today at 2pm? | Fairly true |
| | 23/05/2007 | True Location | How true was the response from Adam when he said he was at the gym today at 5pm? | True |
| | 24/05/2007 | False Location | How true was the response from Adam when he said he was at Bletchley today at 11am? | Very true |
| | 24/05/2007 | False Location plus Activity | How true was the response from Mark when he said he was shopping at Bletchley today at 11am? | Fairly true |

| | | | | |
|---|---|---|---|---|
| | 25/05/2007 | True Location plus Activity | How true was the response from Mark when he said he was at home today doing the dishes at 8am? | Very true |
| | 25/05/2007 | Blurred Location | How true was the response from Adam when he said he was at the City Centre today at 9am? | Very true |
| | 26/05/2007 | True Location | How true was the response from Mark when he said he was at Walton Hall today at 9am? | True |
| | 26/05/2007 | False Location | How true was the response from Adam when he said he was at home today at 8:15am? | Very true |
| | 26/05/2007 | False Location plus Activity | How true was the response from Adam when he said he was window shopping at Kingston today at 11am? | Fairly true |
| | 26/05/2007 | True Location plus Activity | How true was the response from Mark when he said he was at Tesco doing some shopping today at 2pm? | Very true |
| | 27/05/2007 | Blurred Location | How true was the response from Mark when he said he was at Kingston today at 5pm? | Very true |
| | 27/05/2007 | True Location | How true was the response from Adam when he said he was at home today at 11am? | True |
| | 27/05/2007 | False Location | How true was the response from Adam when he said he was at Bletchley today at 2:15pm? | Very true |
| | 27/05/2007 | False Location plus Activity | How true was the response from Mark when he said he was playing football at Walton Hall today at | Fairly true |

| | | | | |
|---|---|---|---|---|
| | | | 11:15am? | |
| | 28/05/2007 | True Location plus Activity | How true was the response from Adam when he said he was watching TV at home today at 8:00am? | Very true |
| | 28/05/2007 | Blurred Location | How true was the response from Mark when he said he was at Bletchley today at 8:15am? | Very true |
| | 29/05/2007 | True Location | How true was the response from Mark when he said he was at home today at 8am? | True |
| | 29/05/2007 | False Location | How true was the response from Adam when he said he was at the City Centre today at 8:05am? | Very true |
| | 30/05/2007 | False Location plus Activity | How true was the response from Adam when he said he was at home watching TV today at 8:15am? | Fairly true |
| | 30/05/2007 | True Location plus Activity | How true was the response from Mark when he said he was at the City Centre today at 11am? | Very true |
| | 31/05/2007 | Blurred Location | How true was the response from Mark when he said he was at Tesco doing some shopping today at 2pm? | Very true |
| | 31/05/2007 | True Location | How true was the response from Adam when he said he was at the gym today at 5pm? | True |
| | 01/06/2007 | False Location | How true was the response from Adam when he said he was at Bletchley today at 11am? | Very true |
| | 01/06/2007 | False Location plus Activity | How true was the response from Mark when he said he was shopping at Bletchley today at 11am? | Fairly true |

| | | | | |
|---|---|---|---|---|
| | 02/06/2007 | True Location plus Activity | How true was the response from Mark when he said he was at home today doing the dishes at 8am? | Very true |
| | 02/06/2007 | Blurred Location | How true was the response from Adam when he said he was at the City Centre today at 9am? | Very true |
| | 02/06/2007 | True Location | How true was the response from Mark when he said he was at Walton Hall today at 9am? | True |
| | 02/06/2007 | False Location | How true was the response from Adam when he said he was at home today at 8:15am? | Very true |
| | 03/06/2007 | False Location plus Activity | How true was the response from Adam when he said he was window shopping at Kingston today at 11am? | Fairly true |
| | 03/06/2007 | True Location plus Activity | How true was the response from Mark when he said he was at Tesco doing some shopping today at 2pm? | Very true |
| | 03/06/2007 | Blurred Location | How true was the response from Mark when he said he was at Kingston today at 5pm? | Very true |
| **Requestor 2** | 21/05/2007 | True Location | How true was the response from Mark when he said he was at home today at 8am? | Very true |
| | 21/05/2007 | False Location | How true was the response from Adam when he said he was at the City Centre today at 8:05am? | Very true |
| | 22/05/2007 | False Location plus Activity | How true was the response from Adam when he said he was at home watching TV today at 8:15am? | Fairly true |

| | | | | |
|---|---|---|---|---|
| | 22/05/2007 | Blurred Location | How true was the response from Mark when he said he was at the City Centre today at 11am? | Very true |
| | 23/05/2007 | True Location plus Activity | How true was the response from Mark when he said he was at Tesco doing some shopping today at 2pm? | Very true |
| | 23/05/2007 | True Location | How true was the response from Adam when he said he was at the gym today at 5pm? | True |
| | 24/05/2007 | False Location | How true was the response from Adam when he said he was at Bletchley today at 11am? | Very true |
| | 24/05/2007 | False Location plus Activity | How true was the response from Mark when he said he was shopping at Bletchley today at 11am? | Fairly true |
| | 25/05/2007 | True Location plus Activity | How true was the response from Mark when he said he was at home today doing the dishes at 8am? | Very true |
| | 25/05/2007 | Blurred Location | How true was the response from Adam when he said he was at the City Centre today at 9am? | Very true |
| | 26/05/2007 | True Location | How true was the response from Mark when he said he was at Walton Hall today at 9am? | True |
| | 26/05/2007 | False Location | How true was the response from Adam when he said he was at home today at 8:15am? | Very true |
| | 26/05/2007 | False Location plus Activity | How true was the response from Adam when he said he was window shopping | Fairly true |

| | | | | |
|---|---|---|---|---|
| | | | at Kingston today at 11am? | |
| | 26/05/2007 | True Location plus Activity | How true was the response from Mark when he said he was at Tesco doing some shopping today at 2pm? | True |
| | 27/05/2007 | Blurred Location | How true was the response from Mark when he said he was at Kingston today at 5pm? | Very true |
| | 27/05/2007 | True Location | How true was the response from Adam when he said he was at home today at 11am? | True |
| | 27/05/2007 | False Location | How true was the response from Adam when he said he was at Bletchley today at 2:15pm? | Very true |
| | 27/05/2007 | False Location plus Activity | How true was the response from Mark when he said he was playing football at Walton Hall today at 11:15am? | True |
| | 28/05/2007 | True Location plus Activity | How true was the response from Adam when he said he was watching TV at home today at 8:00am? | True |
| | 28/05/2007 | Blurred Location | How true was the response from Mark when he said he was at Bletchley today at 8:15am? | Very true |
| | 29/05/2007 | True Location | How true was the response from Mark when he said he was at home today at 8am? | Very true |
| | 29/05/2007 | False Location | How true was the response from Adam when he said he was at the City Centre today at 8:05am? | Very true |
| | 30/05/2007 | False Location plus Activity | How true was the response from Adam when he said he was at home watching TV today at 8:15am? | True |

| | | | | |
|---|---|---|---|---|
| | 30/05/2007 | True Location plus Activity | How true was the response from Mark when he said he was at the City Centre today at 11am? | True |
| | 31/05/2007 | Blurred Location | How true was the response from Mark when he said he was at Tesco doing some shopping today at 2pm? | Very true |
| | 31/05/2007 | True Location | How true was the response from Adam when he said he was at the gym today at 5pm? | True |
| | 01/06/2007 | False Location | How true was the response from Adam when he said he was at Bletchley today at 11am? | True |
| | 01/06/2007 | False Location plus Activity | How true was the response from Mark when he said he was shopping at Bletchley today at 11am? | True |
| | 02/06/2007 | True Location plus Activity | How true was the response from Mark when he said he was at home today doing the dishes at 8am? | True |
| | 02/06/2007 | Blurred Location | How true was the response from Adam when he said he was at the City Centre today at 9am? | Very true |
| | 02/06/2007 | True Location | How true was the response from Mark when he said he was at Walton Hall today at 9am? | True |
| | 02/06/2007 | False Location | How true was the response from Adam when he said he was at home today at 8:15am? | True |
| | 03/06/2007 | False Location plus Activity | How true was the response from Adam when he said he was window shopping | True |

| | | | | |
|---|---|---|---|---|
| | | | at Kingston today at 11am? | |
| | 03/06/2007 | True Location plus Activity | How true was the response from Mark when he said he was at Tesco doing some shopping today at 2pm? | True |
| | 03/06/2007 | Blurred Location | How true was the response from Mark when he said he was at Kingston today at 5pm? | Very true |

# *Appendix E: User Consent and Post Study Questionnaires*

**User Study Instructions for Mobile Client Evaluation**

Thank you for responding to our request for help with our evaluation. This study is hosted by Karim Adam, a PhD student at the Open University Computing Research Centre.

We are conducting research into the use of various techniques to control privacy as it relates to your mobile phone. In particular we are interested in how people can control the disclosure of their location and the ways in which they might need to provide false or imprecise information.

We have built the Mobile Client application to help people better manage their location information. Throughout the two week period that you will be assisting us in this study, you will be provided with phones which have Mobile Client installed on them.
You can use your own SIM card in the new phones provided. In addition, you will be given free airtime credits for the duration of the study.
A demonstration of the functionality of the application will be made to you once you sign the consent forms provided. These include making a request, a disclosure, setting disclosure preferences, and adding contacts.
Each day, you will be sent an alert as to what task to carry out that day. Do not let your friend know what instructions you have been given for your task of the day.

Should you have any queries relating to this study, contact Karim Adam on 07944691540 or k.a.adam@open.ac.uk.

**Mobile Feedback Task Alerts**

The following are alerts that were sent out to disclosers as specific instructions for the various strategies employed in response to a location request.

**Run Mobile Client Alert:**

1. This is a reminder: Could you please start Mobile Client if it's not already running? Thanks for your attention.

**Disclosure Strategy Alerts:**

- Your task today is to disclose your **true location** AND **an activity**. e.g. "home, doing the dishes"

- Your task today is to disclose your **true location**, e.g. "Refectory, Open University"

- Your task today is to disclose an **untrue location** AND include **an activity**. e.g. instead of "office", say "home, watching TV"

- Your task today is to disclose an **explicitly untrue location**, e.g. instead of "Tesco" say "Asda"

- Your task today is to **blur** your disclosed location or make it less specific, e.g. instead of "Office", say "Milton Keynes"

3. Please select the disclosure preference you set today?

- blur my loc
- false loc
- false loc + activity
- true loc
- true loc + activity

4. How true did u find the disclosed location in today's task?

- very true
- true
- fairly true
- not true
- can't tell

**Post Study Questionnaire**

Thank you for successfully taking part in the evaluation of the Mobile Client application. Please take your time to provide your input to the following questionnaire.

GENERIC QUESTIONS (TO ALL PARTICIPANTS)

1. Did you encounter any problems during the two week evaluation period? If yes, please state the nature of the problem in the space provided below:

……..

…….

……

2. If you answered yes above, please suggest (if any) how you would have liked the Mobile Client application to function in order to prevent the problem from occurring.

……

…….

……

3. If your phone had the Mobile Client application with the same capability of helping you manage the amount of location information disclosed to your friends, how useful do you think it would be in protecting your location privacy? Please circle or mark as appropriate.

    a. Very useful

    b. Useful

    c. Somewhat useful

    d. Not at all useful

    e. Cannot tell

## Investigating location privacy in mobile devices

### Informed Consent Form

All of the information obtained from your participation will be kept confidential. Your consent form will be kept separate from the data and the data will not be available to anyone other than the experimenters conducting the study.

You are reminded that your participation is voluntary. This means that you can choose to stop at any time without penalty.

If you have any questions or concerns related to your participation in this study, please call Karim Adam, Department of Computing on 07944691540 or k.a.adam@open.ac.uk.

---

"I have read the information about the study and have been informed of its general purpose. I am fully aware of the risks and benefits associated with participating in the study described to me. I acknowledge that I have received a copy of the informed consent form and agree to participate in the study. I understand that I can withdraw at any time without penalty."

_____ _____

Print name Today's Date

_____

Signature

_____

ID#