


8-2003

User Controlled Privacy Protection in Location-Based Services

Anuket Bhaduri

Follow this and additional works at: <http://digitalcommons.library.umaine.edu/etd>

 Part of the [Geographic Information Sciences Commons](#), and the [Software Engineering Commons](#)

Recommended Citation

Bhaduri, Anuket, "User Controlled Privacy Protection in Location-Based Services" (2003). *Electronic Theses and Dissertations*. 580.
<http://digitalcommons.library.umaine.edu/etd/580>

This Open-Access Thesis is brought to you for free and open access by DigitalCommons@UMaine. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of DigitalCommons@UMaine.

**USER CONTROLLED PRIVACY PROTECTION
IN LOCATION-BASED SERVICES**

By

Anuket Bhaduri

B.S. University of Maine, 2001

B.A. University of Maine, 2003

A THESIS

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

(in Spatial Information Science and Engineering)

The Graduate School

The University of Maine

August, 2003

Advisory Committee:

Harlan J. Onsrud, Professor of Spatial Information Science and Engineering, Advisor

Silvia Nittel, Assistant Professor of Spatial Information Science and Engineering

David Steiger, Associate Professor of Management Information Systems

© 2003 Anuket Bhaduri

All Rights Reserved

USER CONTROLLED PRIVACY PROTECTION IN LOCATION-BASED SERVICES

By Anuket Bhaduri

Thesis Advisor: Dr Harlan J. Onsrud

An Abstract of the Thesis Presented
in Partial Fulfillment of the Requirements for the
Degree of Master of Science
(in Spatial Information Science and Engineering)
August, 2003

The rapid development of location-determining technologies has enabled tracking of people or objects more accurately than ever before and the volume and extent of tracking has increased dramatically over time. Within the broader domain of tracking technologies, location-based services (LBS) are a subset of capabilities that allow users to access information relative to their own physical location. However, the personal location information generated by such technologies is at risk of being misused or abused unless protection capabilities are built into the design of such systems. These concerns may ultimately prevent society from achieving the broad range of benefits that otherwise would be available to consumers. The assumption of the emerging location-based industry is that corporations will own and control location and other information about individuals. Traditionally, privacy has been addressed through minimum standard approaches. However, regulatory and technological approaches focused on “one size fits all” standards are ill equipped to accommodate the interests of individuals or broad groups of users.

This research explores the possibility of developing an approach for protecting privacy in the use of location-based services that supports the autonomy of an individual through a combined technological and legal model that places the power to protect location privacy in the hands of consumers. A proof of concept user interface to illustrate how personal information privacy could be protected in the conceptual model is demonstrated. A major goal of this project is to create an operational vision supporting user controlled protection of privacy that can help direct technological efforts along appropriate paths.

ACKNOWLEDGEMENTS

I would like to thank my advisor Dr. Harlan Onsrud for giving me the opportunity to pursue this project as well as his support, guidance and patience. I would also like to express my sincere thanks to my advisory committee members, Dr. David Steiger and Dr. Silvia Nittel. I am very grateful to the faculty, staff and all my colleagues in the Department of Spatial Information Science & Engineering, especially Sharad, Hari, Farhan, Vijay, Chitra, Mike, Paul, Chris, Greg, Tommy, Dominik and others.

I would like to mention all my friends and acquaintances in Maine and in India, they have been very important to me. This list is endless, but Evan, Prashanth, Daman, Nakib, Babu, Minal, Kamal, Poppin, Micka, Vickey, Bijal, Harsh, Paresh and many others deserve a lot of credit. I am also obliged for the assistance received from the University of Maine, Office of International Programs, Maine Business School, the Department of Economics and the overall University community. Special mention goes to Karen, James, Mereille, Dr. Borgman, Dr. Strong, Dr. Kearney and the people at Stewart Commons and the Computer Connection.

Finally, I would like to convey my most heartfelt thanks to my parents, sister, grandmother, aunt, uncle and the rest of my family for their love, support and encouragement; it has been most instrumental to my success. And thanks to my girlfriend Carleena for standing by and helping me through everything.

This work is partially supported by grant # NMA 201-01-1-2003. This support is gratefully acknowledged.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	iii
LIST OF TABLES.....	ix
LIST OF FIGURES.....	x
Chapter	
1. INTRODUCTION.....	1
1.1 LBS Environments.....	2
1.2 Motivation of Research.....	3
1.3 The Current Situation.....	4
1.4 Basics of User Controlled Privacy Protection.....	6
1.5 Static Standards versus a Dynamic User Controlled Approach.....	7
1.6 Important Questions in Adopting the Proposed Dynamic Approach.....	8
1.7 Some Key Concepts.....	9
1.8 Outline of the Thesis.....	10
2. LOCATION-BASED SERVICES.....	12
2.1 A Basic Definition.....	12
2.2 The Presence of LBS and E-911.....	13
2.3 User Hardware for LBS.....	14
2.3.1 Cell Phones.....	15
2.3.2 Personal Digital Assistants (PDA).....	15
2.3.3 Vehicle Mounted Devices.....	16
2.3.4 The Personal Communicator.....	17

2.4 Location Fixing and Position Determining Equipment.....	18
2.4.1 Triangulation.....	18
2.4.2 Satellite Based Methods for Location Fixing.....	19
2.4.2.1 GPS.....	20
2.4.2.2 E-OTD.....	21
2.4.3 Terrestrial Based Methods for Location Fixing.....	22
2.4.3.1 Cell Global Identity (CGI-TA).....	22
2.4.3.2 Time of Arrival (TOA).....	23
2.4.3.3 Angle of Arrival (AOA).....	23
2.5 Location Aware Servers and Operations.....	24
2.5.1 GeoCoding.....	25
2.5.2 Map Content.....	25
2.5.3 Proximity Searching.....	25
2.5.4 Routing.....	25
2.6 Some Applications of LBS.....	26
2.6.1 Navigation Information.....	27
2.6.2 Travel Guide.....	27
2.6.3 Mobile Commerce.....	28
2.6.4 Emergency Services.....	29
2.6.5 Tracking Services.....	30
3. PRIVACY AND LBS.....	32
3.1 General Introduction to Technology and Privacy.....	32
3.2 Privacy and LBS Environments.....	35

3.2.1	Assessment of Privacy Risks in LBS.....	36
3.3	Prior Approaches for Privacy Protection in LBS.....	40
3.3.1	Platform for Privacy Preferences.....	41
3.3.2	The IETF Geo Privacy Internet Draft.....	42
3.3.3	Overview of LIF Privacy Guidelines.....	45
3.3.3.1	Definitions.....	46
3.3.3.2	LIF Privacy Model.....	47
4.	USER CONTROLLED PRIVACY PROTECTION IN LBS.....	51
4.1	Introduction.....	51
4.2	User Controlled Privacy Protection Model.....	52
4.2.1	Definitions and Architecture of the Approach.....	52
4.2.2	Functions of the “Personal Communicator”.....	53
4.2.3	A Model Contract Approach for Location Privacy in LBS.....	56
4.2.4	Settings of the “Personal Communicator”.....	57
4.2.5	Off Condition Privacy Preferences.....	59
4.2.6	Emergency Response Preferences.....	60
4.2.7	User Specified Communication List Privacy Preferences.....	60
4.2.7.1	User Specified Lists.....	62
4.2.7.2	Privacy Preferences for List of Business Associates.....	63
4.2.7.3	Anyone in the World Privacy Preferences.....	64
4.2.8	Clients of Server Privacy Preferences.....	65
4.2.9	User as Consumer.....	66
4.2.10	Server Privacy Preferences.....	67

4.3 Conflicts in Privacy Preferences: An Operational Example.....	70
4.4 Summary.....	71
5. FURTHER ANALYSIS OF THE MODEL.....	73
5.1 Key Questions.....	74
5.1.1 Pricing Model.....	74
5.1.2 Putting a Monetary Price on Privacy.....	75
5.1.3 Moral Significance of the Model.....	76
5.1.4 Gravitation Towards Lower Prices.....	76
5.1.5 Archiving Preference Status.....	77
5.1.6 Enticing the LBS Industry to Adopt Such a Model.....	77
5.2 Other Issues.....	79
5.2.1 User Education.....	79
5.2.2 Distributing Control over Data.....	80
5.2.3 Technological Feasibility.....	81
5.2.4 Security.....	83
5.2.5 False Information.....	83
5.3 Summary.....	84
6. CONCLUSIONS AND FUTURE WORK.....	85
6.1 Thesis Summary.....	85
6.2 Thesis Conclusions.....	86
6.3 Future Work.....	86
6.3.1 Uncertainty and Mobile Object Databases.....	87
6.3.1.1 Strategies for Handling Uncertainty in MODs.....	88

6.3.1.2 Other Considerations in Mobile Object Databases.....	90
6.3.2 Ubiquitous Computing.....	90
6.3.3 Sensors and Privacy.....	91
6.4 Final Words.....	92
REFERENCES.....	94
APPENDIX A Privacy Laws.....	103
APPENDIX B Code for Mock Up Software.....	108
BIOGRAPHY OF THE AUTHOR.....	117

LIST OF TABLES

Table 3.1: Government Privacy.....	33
Table 3.2: Commercial Privacy.....	34
Table 5.1: A Hypothetical Cost Structure.....	79

LIST OF FIGURES

Figure 2.1: A Typical LBS Application in a PDA.....	16
Figure 2.2: A Vehicle Mounted Device.....	17
Figure 2.3: The Personal Communicator.....	18
Figure 2.4: Handheld LBS Products.....	18
Figure 2.5: Triangulation.....	19
Figure 2.6: GPS Satellites.....	21
Figure 2.7: A Snapshot of LBS.....	24
Figure 2.8: Some LBS Applications.....	26
Figure 2.9: A LBS Map Display.....	28
Figure 4.1: Architecture of the “User Controlled Privacy Model”.....	53
Figure 4.2: The Personal Communicators Main Menu.....	54
Figure 4.3: An Example of a Phone in the Personal Communicator.....	56
Figure 4.4: Privacy Preferences Menu.....	58
Figure 4.5: Off Condition Privacy Preference.....	59
Figure 4.6: Emergency Response Preferences.....	60
Figure 4.7: Communication List Privacy Preferences.....	61
Figure 4.8: List of Business Associates.....	62
Figure 4.9: Privacy Preferences for List of Business Associates.....	63
Figure 4.10: Anyone in the World Privacy Preferences.....	64
Figure 4.11: Clients of Server Privacy Preferences.....	66
Figure 4.12: User as Consumer Preference Menu.....	67

Figure 4.13: Server Privacy Preferences.....	68
Figure 4.14: Server Privacy Preferences (Page 2).....	69
Figure 6.1: Uncertainty in Location.....	87
Figure 6.2: A Bayesian Networks Example.....	89

CHAPTER 1

INTRODUCTION

What research challenges would scientists be pursuing and what would be the direction of development if scientists and developers treated morality as the ultimate determiner in directing their technological knowledge advancement efforts (Onsrud 2003)? The rapid development of location-determining technologies has enabled tracking of people or objects more accurately than ever before and the volume and extent of tracking has increased dramatically over time. Tracking technologies will continue to expand in use and it is very important for the technologies to adapt to the technological and social needs, desires, and expectations of users and to the needs of society as a whole. Within the broader domain of tracking technologies, location-based services (LBS) are a subset of capabilities that allow users to access information relative to their own physical location. The personal location information generated by such technologies is at risk of being misused or abused unless protection capabilities are built into the design of such systems (Onsrud 2001). Kant and other philosophers have steadfastly argued that a key element of being a person is one's ability to be *autonomous* or self-defining. According to Kant, coercion and deception are the most basic of wrongdoing to others since they deprive the individual of assent. Yet, the strong assumption of the emerging location-based industry is that corporations will own and control location and other information about individuals. They will decide what levels of privacy protection to provide based on pragmatic considerations, such as obeying the law and responding to marketplace dynamics (Onsrud 2003).

The primary hypothesis of this thesis is that *it is possible to develop an approach for protecting privacy in the use of location-based services that supports the core ethical principle of autonomy of the individual*. This hypothesis is tested, not by providing an operational system, but by developing a combined legal and technological *conceptual model* that places the power to protect location privacy in the hands of consumers of location-based services (Onsrud 2003). The model establishes a vision for a future comprehensive technological LBS capability. A proof of concept user interface to illustrate how personal information privacy could be protected in the conceptual model is demonstrated.

1.1 LBS Environments

“Location-based services are services that exploit knowledge about where an information device or user is located” (TechTarget 2001). The advent of high bandwidth wireless networks has helped stimulate the growth of location-based services. They have become increasingly popular over the past few years. More and more people are subscribing to such services in order to obtain geographically based information about facilities and activities of interest to their own tasks or objectives. Geographic Information Systems (GIS) and Global Positioning Systems (GPS) have been stepping-stone technologies for the development of location-based services. The most common methods of accessing and subscribing to LBS are through mobile handheld devices and vehicle mounted devices. By example, today’s LBS users might typically seek locations and information about restaurants, businesses, gas stations and similar commercial establishments (Bhaduri and Onsrud 2002).

1.2 Motivation of Research

In addition to use by consumers, the location data from these new tracking systems are becoming available for use by third parties with whom the user does not have a direct relationship (Clarke 1999). The ability of the location-based service provider to collect location specific data on individuals has raised many personal information privacy concerns. These concerns may ultimately hinder industry in delivering the broad range of benefits that otherwise would be available to consumers. The information amassed through the use of LBS gives service providers the ability to sell location information identifiable to individuals to third parties for financial gain. In most cases such activities are unknown to the user (Dobson 1998). Under the current state of technology, subscribers are left in the vulnerable position of not having control of their own location information. Most examples of how LBS might benefit consumers raise issues of information privacy risk as well. To show how relevant location-based advertising could be, advertisers used the example of a shopper receiving a coupon for fifty cents off a double non-fat latte on his mobile device while walking by a gourmet coffee shop (Gutzman 2001). Privacy-industry representatives used the same example to show how intrusive such technologies could be (Gutzman 2001). Hence, both the benefits and drawbacks are readily apparent to most potential users. Traditionally privacy has been addressed through policy-based or legal standard approaches. These approaches establish minimum standards for protection performance by industry but typically do not protect information to the extent that consumers desire and are comfortable with. Such approaches also are applied with a broad brush (Onsrud 2001). Laws focused on specific minimum standards are not suited for ensuring that each person is able to choose the level

of privacy that he or she desires. Technology and social conditions change rapidly, and *one-size-fits-all* standards are unable to quickly or accurately accommodate the interests of each individual or broad groups of users (Onsrud 2001).

1.3 The Current Situation

Federal laws govern the use of available location information in case of an emergency and service providers are required to provide the information as accurately as possible under the E-911 mandate (FCC 2001). Various laws also afford a certain level of minimum privacy protection to individuals that should not be breached. By example, a persons medical records are usually off limits for commercial use. Most rational people are not opposed to providing location information in case of an emergency, but the possibility of using this information for other purposes raises cautionary flags for most privacy advocates. Consumers are concerned about the potential impact of location-based services on personal information and location privacy (Gidari 2000). This also includes threats to personal security and the use of personal location records for commercial purposes. By example, subscribers purchasing an LBS service may be hard pressed to avoid unwanted solicitations and intrusions. In order for spatial technologies such as LBS to be more acceptable and adaptable for use in e-commerce and society in general, privacy considerations need to be accounted for from the outset in the design and coding of such systems (Onsrud 2001).

Current mandatory or recommended standards for information privacy protection are established through federal and state legislatures, industrial collaboration committees, consumer organizations and privacy advocates, but not by individual consumers on an

ongoing basis (Gidari 2000). On most occasions, a subset of the above mentioned groups get together on a periodic basis and arrive at a recommended or mandated level of privacy that should be afforded to users. The involved parties typically try their best to arrive at a level of privacy protection that most stakeholders can live with. However, the approach is often subject to considerable sway by those at the table. Vested interests involved in standard setting typically do not have the welfare of individual users or the economic well being of the entire industry as paramount concerns. For example, businesses typically advocate for maximum control over consumer location information to provide flexibility in experimenting with revenue generation options. Privacy advocates on the other hand typically advocate for minimum retention of location information by the commercial sector even though more extensive retention might be of great value to specific users requesting a service and might provide greater profitability to the economy as a whole. It is almost impossible to achieve a middle ground that will satisfy most of the affected parties most of the time (Onsrud 2001). The amount of privacy preferred is different for different people and changes with each individual over time. One person might demand complete privacy and another might be indifferent towards detailed information about their activities being tracked by others. A person might want less privacy when he or she is not busy, but during working hours they may prefer to be left alone. A person might feel secure and see little need for privacy protection one week but during a crime spree in their community the next week want to minimize their information exposure. The current institutional and governmental systems for protecting privacy are static. They are only changed when there is an explicit update or change in corporate or industry policy or perhaps a change in privacy legislation

(Bhaduri and Onsrud 2002). *One-size-fits-all* privacy protection is both economically and socially inefficient since the ability to adapt to specific circumstances is non-existent. An approach that is flexible enough to respond to consumer desires and marketplace conditions while maintaining base level minimum protections would be far more beneficial for individuals, the commercial sector, and society as a whole.

1.4 Basics of User Controlled Privacy Protection

The alternative we propose is a combined technological and legal model that places the power to protect location privacy in the hands of consumers of location-based services rather than in the hands of service providers. This is a dynamic approach that distributes control between users and service providers based on continuous contracts, which are integrated into the technology of the LBS environment (Bhaduri and Onsrud 2002). Pursuit of this alternative could help bolster the robustness of location-based service environments and make them more attractive to consumers. The contract-based model addresses issues such as who controls the location information, how accurately service providers may track moving objects, how long service providers may retain personal data, whether entities other than the service provider may have access to the location data, and several other areas of concern. We address the cost of such a model, keeping in mind that there is a need to consider the technological cost of communication and computational operations as well as the monetary costs behind implementing such a ground-up system. Depending on the specific application, uncertainty and location prediction of moving objects are also challenging conceptual and software design issues that may hinder practical implementations of the proposed model (Sistla, Wolfson et al

1997). The automated system for implementing continually changing contract terms and the archiving of past contract terms also require a deal of attention. One goal of this project is to create an operational vision that supports user-controlled protection of privacy that can help direct technological efforts along appropriate paths. Service providers have an incentive to pursue such a contract-based approach if they are able to capture a market that otherwise would never take up or would be slow to take up location-based services. We explore both the benefits and drawbacks of the conceived model in this research. All the issues mentioned in the above section are dealt with individually and collectively throughout this research project.

1.5 Static Standards versus a Dynamic User Controlled Approach

A fair amount of material is available on the issue of location privacy with respect to minimum standard or policy based approaches. An entire chapter devoted to the merits and demerits of some of these approaches is included further in this work. By example, one substantial effort is the work undertaken by the Internet Engineering Task Forces (IETF) Geo-Privacy group (Cuellar 2002). In contrast, our dynamic approach is based on an opt-in/opt-out method that provides users with the opportunity to actively select or deselect the time and purpose of the use of any information. Users have the option of providing themselves with as little or as much privacy protection as they desire although minimum levels of privacy protection as mandated by law or accepted by the industry can also be supported. Developing a system that protects personal privacy responsive to individual desires is essential to further public interest in developing spatial technologies such as LBS. Accountability and enforcement of privacy rules set by users are necessary

to bolster consumer confidence (Wang, Lee et al 1998). Mobile location services that provide users with greater flexibility and direct control over protecting their own personal information and location privacy are likely to grow more quickly and become the most successful services in the marketplace. Business and service providers willing to relinquish control over their clients' location information should be able to grow more quickly and robustly their primary service market for delivery of location-based services in exchange for giving up speculative revenues from secondary markets. LBS businesses need to have a core market acquiring their services before they can have a secondary market for the sale of personal information. Consumers have all experienced the intrusiveness of unwanted marketing over their phones. It is the threat that even more intrusive activities will occur in the LBS industry that will keep buyers and subscribers away. Thus, the knowledge that intrusive tracking will occur is a major hindrance to development of a primary market for LBS. It is our hope that this research will catalyze the marketplace and others to explore alternative ways of thinking about privacy protection. The focus of our attention is on location tracking but we believe the dynamic contract-based technological solution described may have broad ranging applicability in other information privacy-threat technological environments (Bhaduri and Onsrud 2002).

1.6 Important Questions in Adopting the Proposed Dynamic Approach

What kinds of economic practices and pricing models will likely result from the proposed approach? Will the developed systems result in greater privacy protection for those who pay more? Is greater autonomy for each individual a morally appropriate design choice when in practice poorer people may have less choice than wealthy users?

Will everyone in society in practice gravitate towards the lowest price and therefore the lowest privacy protection? When the user-defined contract allows the service provider to pass on location information about the user, should there be any limitations on the use by third parties beyond that proscribed by the legal system? For the ever-changing contractual relationships, how should the technology manage the status of the contract and the automatic enforcement of the contract provisions? Must an archival record be kept of all past user preference status conditions? What conditions will entice industry to adopt user-controlled dynamic privacy preference approaches? Many of the issues raised by the above questions are discussed, although not necessarily resolved, in the sections that follow.

1.7 Some Key Concepts

Before we continue on to any specific chapters it is important to clear up some basic definitions.

Location is a description of an entity's whereabouts, in relation to other, known objects or reference frameworks. Location can be ascertained with varying degrees of precision (Clarke 1999).

Tracking is the plotting of the trail or sequence of locations that is followed by an entity within a space over a period of time. The 'space' within which an entity's location is tracked is generally physical or geographical; but it may be virtual, e.g. a person's successive interactions with a particular organization (Clarke 1999).

Target is a mobile electronic device that may be tracked by location (Cuellar 2002)

User is person associated with a specific target (Cuellar 2002).

1.8 Outline of the Thesis

The first chapter has provided a basic introduction to the problem of privacy protection in location-based service environments and outlines the fundamental concepts and key principles in arriving at a new approach for protecting privacy. Chapter 2 provides background information on the technology and applications of location-based services. It discusses related spatial technologies such as GPS and GIS that are prerequisite technologies for LBS. Chapter 3 begins by discussing privacy in general and then in the context of the Internet. The primary focus of the chapter is the effect that location may have on personal information privacy. It also discusses previous and current approaches used to address privacy threats in the use of LBS, including the initiative undertaken by the IETF geo privacy group. It explains the geo privacy group's initiative and outlines the shortcomings of that approach. Chapter 4 introduces our novel proposed solution, which involves user controlled privacy preferences. The model is differentiated from previous approaches, the prototype system is described and the chapter explores many alternatives that can be employed in such a system. The prototype consists of mock up software that demonstrates the concept, but is not a comprehensive implementation of the legal and technological model. This chapter tests the ability to develop a combined legal and technological *conceptual model* that places the power to protect location privacy in the hands of consumers of location-based services. The practicality of the model is tested through a demonstration of how a typical user might interact with a system supporting autonomy of the individual. Chapter 5 details the model and provides proposed solutions for many conceivable privacy preference issues. Its benefits are

questions raised in section 1.6 are addressed in the chapter. It also outlines the limitations of our model and analyzes the technological feasibility to implement the approach. In Chapter 6 the significance of the model and its testing are summarized. Conclusions are presented and future work is suggested.

CHAPTER 2

LOCATION-BASED SERVICES

This chapter presents various definitions, technologies and applications of Location-Based Services (LBS). It is important to understand several logistical and technological considerations before we delve into a detailed privacy model. The following subsections present some of the key concepts integral to LBS, keeping in mind that our eventual goal is achieving a conceptual model to protect information privacy within the domain.

2.1 A Basic Definition

“Location Based Services can be described as applications, which re-act according to a geographic trigger. A Geographic trigger might be the input of a town name, zip code, street or the position of a mobile device user. Providing services based on knowledge of where someone is or where they intend to go is the essence of LBS” (Whereonearth 2001). The user location information in this case consists of X-Y coordinates generated by location determination technology such as Global Positioning Systems (GPS) and Enhanced Observed Time Difference (EOTD) (GeoCanada 2001). A number of these technologies are discussed later in this chapter. In simple terms, using the knowledge of where someone is or where they intend to go is the essence of LBS. This value added service and associated technologies have generated tremendous interest over the past few years (Bennahum 2001). The major purposes to which LBS are applied include emergency response, entertainment, navigation information, tracking and

monitoring, and mobile commerce (Benson 2001). LBS have been around in one form or another for a long time but the arrival of high bandwidth mobile networks has focused a spotlight on their potential. “There is a huge amount of information available which can be re-purposed for the wireless Internet. This coupled with the ability to filter and personalize content by reference to a user's physical location is providing compelling businesses opportunities, which can be fun and also save business money through improved efficiencies” (Whereonearth 2001).

2.2 The Presence of LBS and E-911

The presence of LBS is far more obvious in developed European countries that are able to use the comfortable compatibility of the global system for mobile communication (GSM) standards. The U.S markets also seem to be embracing this technology with open arms. Allied Business Intelligence estimates that the LBS industry will account for more than \$40 billion in revenue by 2006 (TechTarget 2001). Most telecommunications carriers plan to pursue either network- or handset-based location fixing technologies in their networks. Sprint Corporation announced it would incorporate GPS chips into its handsets in 2001 (TechTarget 2001), which could provide a boost to the nascent industry. Several other companies are wrapping up initial LBS and location-relevant wireless advertising test markets. The development of this domain in the U.S was catalyzed by a mandate issued by the Federal Communication Commission (FCC 2001). The FCC has enacted policies that force cell phone and mobile service operators to be able to provide subscribers location data for emergency and safety applications (Gidari 2000).

The wireless Enhanced 911 (E911) rules seek to improve the effectiveness and reliability of wireless 911 services by providing 911 dispatchers with additional information on wireless 911 calls (FCC 2001). The wireless E911 program is divided into two parts - Phase I and Phase II. Phase I requires carriers, upon appropriate request by a local Public Safety Answering Point (PSAP), to report the telephone number of a wireless 911 caller and the location of the antenna that received the call. Phase II requires wireless carriers to provide far more precise location information, within 50 to 100 meters in most cases. The deployment of E911 requires the development of new technologies and upgrades to local 911 services, as well as coordination among public safety agencies, wireless carriers, technology vendors, equipment manufacturers, and local wireless carriers (FCC 2001). The FCC established a four-year rollout schedule for Phase II to be completed by December 31, 2005. The FCC has granted waivers of the Phase II rules to several wireless carriers at the current time. (FCC 2001)

2.3 User Hardware for LBS

Location-based services are delivered currently to users typically through devices such as cell phones, personal digital assistants (PDA's), and vehicle mounted devices. While cell phones and vehicle-mounted devices may connect to services through a cell tower network, a laptop computer or PDA might additionally or alternatively connect through a local area wireless network. *Network Communication Capable Mobile Devices* represent the client side of location-based services and act as the interface for users. LBS subscribers use these devices to obtain information based on geographic location. Such devices are also the objects that are tracked in order to provide the user

with desired information. Each device is equipped with signaling mechanisms that allow service providers to communicate with the device. Typically the LBS device also includes incorporation of a GPS receiver or some other means for locating the device as it moves. GPS capabilities are discussed in the next subsection along with other methods of determining (XYZ) location coordinates. Some of the most common interfaces used for Network Capable Mobile Devices are listed below.

2.3.1 Cell Phones

Over the years, cell phones have become omnipresent in the developed world and have great potential in the developing world. They can now be equipped with many features including multimedia data capabilities and GPS receivers (Bennahum 2001).

2.3.2 Personal Digital Assistants (PDA)

Like cell phones, PDAs are also fairly common, especially among the business community. The fine line between laptop computers and PDAs is slowly disappearing as smaller and faster processors are developed. The continuing improvement in wireless network bandwidth is another major factor that propels PDAs into being a major player in location-based services. Some of the commonly used brand names that already provide wireless modems and GPS receivers are the Palm, Handspring, Ericsson and Compaq series. Figure 2.1 shows an Ericsson PDA used for an LBS application. In this figure, the user is accessing a street map through the provided interface and input device, which in this case is a stylus pen (Ericsson 2003).



Figure 2.1 – A Typical LBS Application in a PDA (Ericsson 2002)

2.3.3 Vehicle Mounted Devices

As the name suggests, these are devices that are usually mounted in cars, trucks, and delivery vehicles (Magellan 2003). They can provide a visual or audio interface and in some instances can be used solely for tracking purposes. One well known and common vehicle-mounted LBS is the Onstar system (Onstar 2003). Figure 2.2 shows a vehicle-mounted device with an interface and an external input controller (Magellan 2003). These LBS environments can be comprised of just a small tracking device or an elaborate setup with multiple input and output devices.



Figure 2.2 – A Vehicle Mounted Device (TechTarget 2001)

2.3.4 The Personal Communicator

Discussion in the remainder of this thesis assumes development of a futuristic *personal communicator* that combines and extends the functionalities of cell phones, PDAs and similar LBS interfaces. Figure 2.3 is from a mock device developed to illustrate concepts of how user controlled privacy protection might be supplied in location-based services. Examples of this personal communicator are used throughout the thesis to explain various details of the developed model. The mock user interface allows illustration of a range of scenarios of user-controlled privacy but is not a functional LBS. Details of the digital mock-up implementation are contained in Chapter 4 and 5. Figure 2.4 shows some current handheld LBS products, these particular ones are equipped with GPS receivers and are used in several field applications (Magellan 2003).

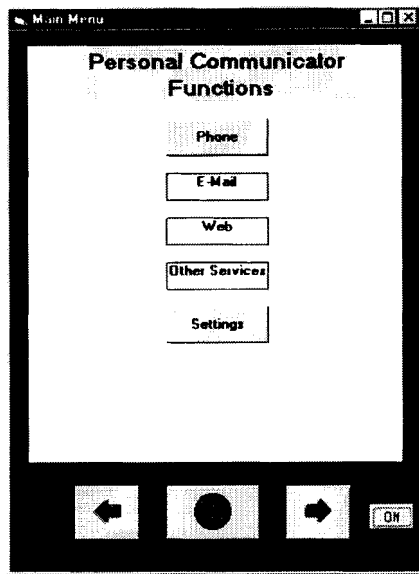


Figure 2.3 – The Personal Communicator



Figure 2.4 – Handheld LBS Products (Magellan 2002)

2.4 Location Fixing and Position Determining Equipment

To understand how the user hardware works requires an understanding of *location fixing* and *location aware servers* and several other key concepts. This subsection discusses some key concepts such as triangulation and various methods of location fixing and certain tangible technologies that are used to fix the location of the above-mentioned mobile devices.

2.4.1 Triangulation

Triangulation is a process by which the location of a radio transmitter can be determined by measuring either the radial distance, or the direction, of the received signal from two or three different points (GeoCanada 2001). Triangulation is sometimes used in cellular communications to pinpoint the geographic position of a user. Figure 2.5 illustrates the basic principle of triangulation. In the illustration shown by the top

drawing, the distance to the cell phone is determined by measuring the relative time delays in the signal from the phone set to three different base stations. In the illustration shown by the bottom drawing, directional antennas at two base stations can be used to pinpoint the location of the cell phone (GeoCanada 2001).

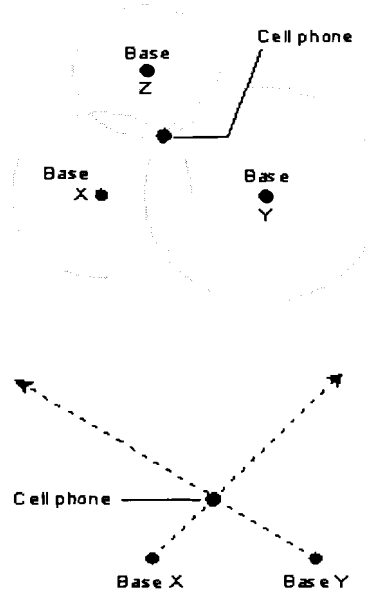


Figure 2.5 – Triangulation (GeoCanada 2001)

2.4.2 Satellite Based Methods for Location Fixing

Satellite based location fixing is widely used by many LBS carriers to provide efficient services to users. The satellites are used along with land based satellite receivers to determine location (TechTarget 2001). New generations of receivers are small enough to be mounted or attached to mobile devices such as cell phones and PDA's. There are two existing global satellite navigation systems and another in development. The U.S. Global Positioning System (GPS), which is far superior to the occasionally unreliable

Russian counterpart GLONASS, is discussed in the next section. The system under development is the European system called Galileo (Mountain, Raper 2001).

2.4.2.1 GPS

The GPS is a "constellation" of 24 well-spaced U.S. satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location (GeoCanada 2001). GPS equipment is widely used in science and has now become sufficiently low-cost so that almost anyone can own a GPS receiver. Figure 2.6 (b) and (c) are pictures of a GPS satellite orbiting the earth, at different times of day. GPS receivers have been used in vehicle navigation systems as well as dedicated handheld devices for some time, and now they are making their way into the mobile Internet (Magellan 2003). With GPS, the mobile device gets positioning information from a number of satellites (usually 3-4). This raw information can then either be processed by the mobile device or sent to the network for processing, to generate the actual position. Figure 2.6(a) illustrates a location being fixed from 4 different GPS satellites. The US government previously distorted the satellite clock signals to reduce accuracy with the Selective Availability (SA) mask; but, that was removed in May 2000 (Mountain, Raper 2001). This means that GPS now achieves around 5m-40m accuracy for most common mobile devices provided there is a clear view of the sky. GPS chipmakers have now reached an increasing level of integration. One-chip solutions are now very power efficient and low cost (GeoCanada 2001).

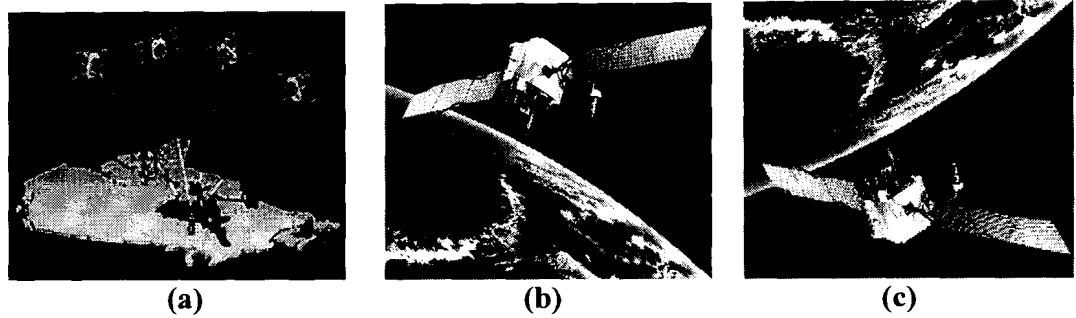


Figure 2.6 – GPS Satellites (GeoCanada 2001)

Another subset called network Assisted GPS or A-GPS uses fixed GPS receivers that are placed at regular intervals, every 200km to 400km on the ground to fetch data that can complement the readings of the mobile device (GeoCanada 2001). The assistance data makes it possible for the receiver to make timing measurements from the satellites without having to decode the actual messages. This assistance greatly reduces the time needed for a GPS receiver to calculate location. Without the assistance information, the Time-to-First-Fix (TTFF) could be in the range of 20-45 seconds (GeoCanada 2001). With assistance data the TTFF is in the range of 1-8 seconds. The assistance data is broadcast around once each 1 hour. So the provision of assistance data imposes little burden on the network while providing great benefit (GeoCanada 2001).

2.4.2.2 E-OTD

Enhanced Observed Time Difference (E-OTD) only uses software in the mobile device. To run the E-OTD algorithms in either idle mode (mobile device is not handling a call) or dedicated mode (mobile device is handling a call), new phones or alternative mobile devices using the phone cell network must be designed with additional processing

power and memory. The E-OTD procedure uses the data received from surrounding base stations to measure the difference it takes for the data to reach the mobile device. That time difference is used to calculate where the user is located relative to the base stations. This requires that the base station positions are known and that the data sent from different sites is synchronized. The most common way of synchronizing the base stations is via the use of fixed GPS receivers. The calculation can then either be done in the mobile device or the network. The accuracy of E-OTD is expected to be around 125m, and unlike GPS it is not reliant on a clear sky above (GeoCanada 2001).

2.4.3 Terrestrial Based Methods for Location Fixing

These methods of location fixing have been around for a while, and they are not nearly as precise as satellite based methods. However, they are still broadly used, especially in cell phones. Many cell phone companies rely on terrestrial based methods to accommodate E-911 (TechTarget 2001). The basic principles of triangulation are extremely important and apply in some form in all the methods listed below.

2.4.3.1 Cell Global Identity (CGI-TA)

This uses the identity of each cell (coverage area of a base station) to locate the user. It is often complemented with *timing advance* (TA) information. TA is the measured time between the start of a radio frame and a data burst. This information is already built into the network and the accuracy is satisfactory when the cells are small (a few hundred meters). For services where proximity (show me a restaurant in this area) is the desired information, this is a very inexpensive and useful method. It works with all

existing mobile devices, which is a big advantage. The accuracy is dependent on the cell size and varies from 10m (a micro cell in a building) to 500m (in a large outdoors macro cell) (GeoCanada 2001).

2.4.3.2 Time of Arrival (TOA)

The time of arrival (TOA) method works in a very similar way as E-OTD, the difference being that the uplink data is measured (the data that is sent by the mobile device). The base stations measure the time of arrival of data from the terminal. This requires that at least three monitoring base stations are available to perform the measurements. The base stations note the time difference and combine it with absolute time readings using GPS absolute time clocks. E-OTD and TOA might look very similar, but the key difference is that TOA supports legacy mobile devices. This is a crucial aspect, as it will take time to convince all mobile device manufacturers to implement a change in their software. The drawback of TOA is that it requires monitoring equipment to be installed at virtually all of the base stations. This is potentially the most expensive of location procedures for operators to implement (GeoCanada 2001)

2.4.3.3 Angle Of Arrival (AOA)

In this method, the users position is determined by estimating the arrival angle of the signal at the base station. It basically requires a complex antenna array on the tower at each base station (GeoCanada 2001).

2.5 Location Aware Servers and Operations

This is a group of servers that uses the location information attained from the location fixing and processes the client request. It is used in conjunction with the geographic content to provide relevant and useful information to the client (Clarke 1999). These servers contain several layers of GIS and attribute data and are capable of several operations. In other words, they are the software and database systems that provide the service based on location. In a way these are the essence of LBS along with the hardware and location fixing. Figure 2.7 provides some insight into LBS as a whole, by displaying the interconnected parts individually and as a unified system. It illustrates the working of mobile devices with satellites and satellite receivers and computer systems that tie them together. Some of the common operations performed to provide clients with geographically based content are described in the following subsections.

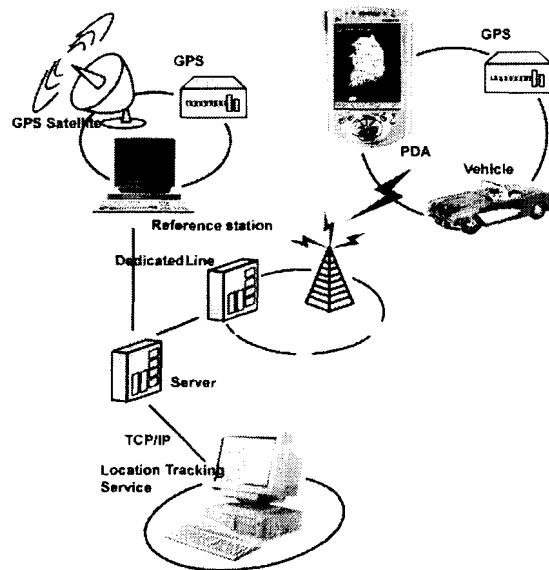


Figure 2.7 – A Snapshot of LBS (TechTarget 2001)

2.5.1 GeoCoding

This is the task of processing textual addresses to add a positional co-ordinate (latitude : longitude) to each address. These co-ordinates are then indexed to enable the addresses to be searched geographically in ways such as "find me my nearest" (Whereonearth2001).

2.5.2 Map Content

This can either be in Raster or Vector format. Raster images are pre-rendered pictures, while vector data is a series of matching layers, each layer contains a specific type of information (a layer for parks, motorways, streets, rivers etc). Both formats can be used to display maps onto a screen (Whereonearth 2001).

2.5.3 Proximity Searching

This is an important element in LBS. It is the method of finding "relevant" information to meet the users specific request. Examples include; "find everything within a radius of...", "select everything I will drive past in the next hour" or "show me where I am" (Whereonearth 2001).

2.5.4 Routing

Routes are calculated by using the users location (origin), a planned destination, and various optimization routines such as shortest distance, most scenic, or fastest route. A resulting chosen route is displayed on a map and *driving directions* are automatically

generated from the route. In case of changing traffic or road situations, traffic data can be merged with the static map content to provide real-time alternative route suggestions and give the driver notice of the adjusted the travel time (Whereonearth 2001).

2.6 Some Applications of LBS

The previous section discussed various operations performed by location aware servers. Operations and applications seem synonymous, but they are somewhat different from each other. Operations in this case are a specific set of tasks executed by computers, in order to provide geographically based content to the user. Applications on the other hand are broader in nature and can be composed of a set of several different operations. Figure 2.8 provides an idea of potential applications of LBS. It illustrates how mobile equipment can be used to obtain services based on location. Among the digital location services that are now being provided as applications or that are likely to be provided in the future include those described below.

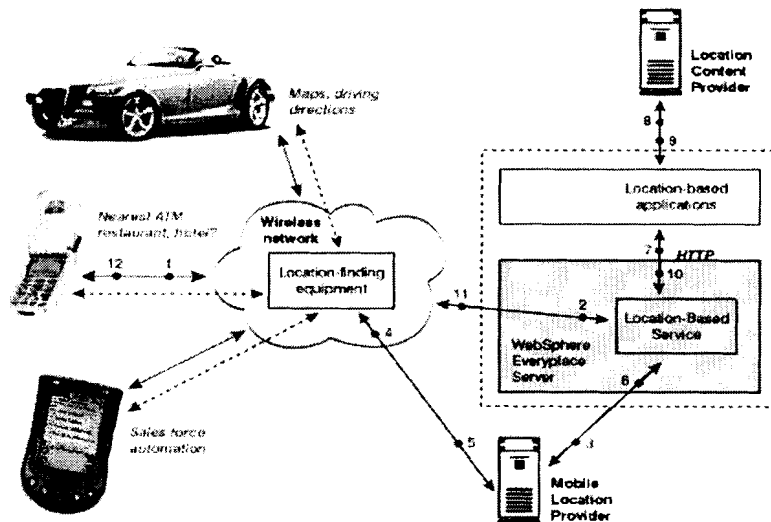


Figure 2.8 – Some LBS Applications (IBM 2002)

2.6.1 Navigation Information

Location-based services have brought significant changes in the way we navigate. The applications of LBS in this domain are plentiful. This advent has dramatically changed our perspective of unknown places, destinations and routes. With a location sensitive service device in our pockets, we can travel around the world; explore destinations without the fear of being lost (Dennis 2001). The use of “Route determination” plays a vital role in navigation information services offered by LBS. Traffic can be one of the biggest problems when running on a busy schedule. By incorporating a *traffic server* that stores up to date traffic information, the LBS could offer ready solutions to relieve traffic delays for the user. It considers the scenario at hand and provides routing computations based on current traffic information (Dennis 2001).

2.6.2 Travel Guide

Digital travel guides are similar to directory services. An example of use would be for a person who wants to go to a movie theater but is unfamiliar with the geographic area. Such a user can immediately query the wireless device for a theater in that area. The server has a series of points of interest (POI's) that may include services such as gas stations, banks, hospitals, restaurants and other services. The device might display a list of customer-oriented retail outlets that fit into the users criteria. It could also carry a local business and entertainment directory for the queried region. Figure 2.9 shows an LBS interface that is displaying a map, based on a query for wineries in a given area (Siemens 2003). By example, a user feels hungry and would like to go to the nearest restaurant. He is not quite sure of his position, so he asks his wireless device to point him to the nearest

possibility. The device takes the users position and searches for restaurants in his proximity. The device can direct the user to a restaurant of his choice, and could also display the route and directions to the destination (Dennis 2001).

Yet another example would be a user asking for directions to a particular place. The user specifies the attributes of the place such as address or phone number. The device transmits to the server, which searches the database and pinpoints the position of the desired location and displays it back to the wireless device. Similar ideas could be used to develop a tour guide. This would aid subscribers in planning tours to their desired destinations and moving in an efficiently planned manner. A travel guide mounted in a car can help drivers navigate with little hassle.

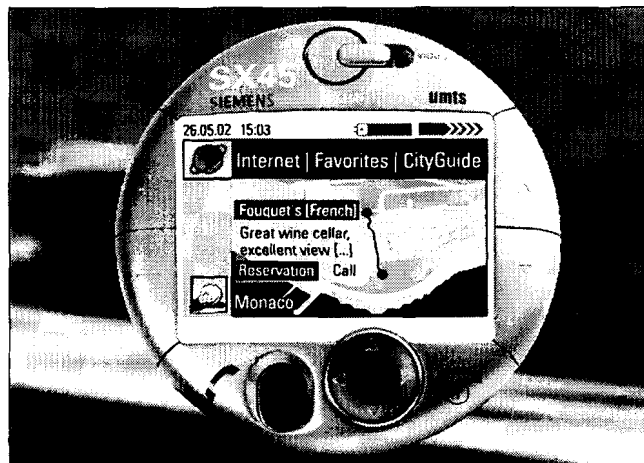


Figure 2.9 – A LBS Map Display (Siemens 2002)

2.6.3 Mobile Commerce

Mobile commerce (M-commerce) is defined as the trading of goods or services through a wireless hand held device. It applies to online financial transactions from shopping to electronic transfer of funds through the mobile device. This introduces a whole new concept of spending money. *Mobile Marketing* is a sub function that is best

explained with the following example. A user walking through a shopping mall suddenly receives a message on his mobile device informing him about a sale for sweaters. The user decides to check the advertising store. He browses through the winter wear section and would now like to check the price listings of winter wear in similar stores. He uses his wireless device to obtain a listing of prices from several different stores. This way he can compare prices on-line, rather than checking out the prices in each store. This is the gist of wireless marketing. Users are notified through a wireless device about services they might be interested in (Dennis 2001). They can also customize the service by having a personalized listing of desired products. *Mobile Payment* is another concept that can be summed up as financial transactions through a wireless device (Dennis 2001). It allows users to key in personal identification numbers, which authenticate the users bank account and authorize transactions. Mobile payment is also capable of enabling stocks and securities transactions through mobile devices.

2.6.4 Emergency Services

As we know from the previous E-911 section, the concept of location-based services originated for use in emergency situations. In the case of an emergency, like a car accident or highway, users are generally unaware of their location. Hence, it was necessary to mandate Enhanced 911 so that the location of the vehicle becomes known. The response time in any emergency is incredibly important and in emergencies such as accidents response time may be the difference between life and death. Thus, in the case of emergencies, determining position of the caller is vital. Calls are received in call receiving centers and the location is noted and passed on to the nearest emergency

response center and appropriate relief is initiated (Gidari 2000). *Automatic Collision Notification* is an emergency service provided by some LBS providers. A device is fitted into cars and other vehicles, once there is a collision, information is sent to appropriate call centers. Based on this data, the call center determines the severity of the crash and tries to establish communication with the vehicle. Once the logistics are quickly handled, appropriate emergency responders are dispatched as per their need (Magellan 2003).

2.6.5 Tracking Services

These services basically answer the question “Where is everything else?” These tracking services are being used increasingly in commercial markets where people like to keep track of their belongings. Examples of these services include taxi companies that would like to track and analyze movements of their taxi drivers. Monitoring these movements helps them police the activities of errant drivers who could potentially misuse the company’s vehicles. Such tracking methods are also commonly exercised by trucking companies to keep tabs on their truck drivers (Magellan 2003). This leads us to the concept called ‘Geo-Fencing’, which refers to an imaginary fence put around an object. If the object leaves this ‘Fence’ the user is immediately informed. Many parents would like to be able to know the activities and whereabouts of young children to prevent them from engaging in undesirable situations or simply for safety purposes. Similarly, pet owners would like to prevent animals from straying away. Stolen vehicles can also be easily tracked using these services.

The potential of location services is limitless and it is possible to list numerous other applications, but the focus of this thesis is privacy in LBS environments. The

introductory and technological groundwork is now set and the next chapter focuses on privacy in location-based services.

CHAPTER 3

PRIVACY AND LBS

The common law definition of "privacy" arose under Supreme Court Justices Warren and Brandeis who defined privacy as " the right to be left alone" (Warren and Brandeis 1890). The Privacy Act of 1974 sets forth a "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies (US Code, Title 5, Sec 552a). However, the Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines leave it open to interpretation and therefore difficult to apply and enforce. It is especially deficient, given the rapid pace of technology. S. Adler defined privacy issues related to telecommunications as: " the right to be disturbed, the right not to be anonymous, the right not to be monitored and the right not to have one's identifying information exploited." (Gattiker et al 1996). Thus, it is apparent current that privacy legislation is generally ill equipped to accommodate emerging technologies such as LBS. The next few sections demonstrate how technology in general and location technologies specifically pose a threat to personal information privacy.

3.1 General Introduction to Technology and Privacy

Both the government and commercial companies are realizing the benefits to be gained by using geographic data sets. Most government agencies justify the need to collect personal data through the mandated missions of their agencies. Their actions are also controlled by privacy legislation. However, with the use of computer technologies

and GIS the potential for misuse is heightened. (Bethell 2002) conducted a survey to gain insight into people's importance on privacy regarding the government and commercial sector. It asked the following questions regarding government privacy:

- Question 1) Information contained in government data sets about the locations of an individual's activities should be kept private.*
Questions 2) Government agencies should be allowed to cross-match data about the past and present locations of individuals in order to accomplish government objectives.

Table 3.1 indicates that most people consider privacy to be a highly important societal goal with regard to government organizations. Most people in this sample seem to believe that data in government databases should be kept private, although the percentages are relatively lower in terms of question 2 being a highly important social goal.

Societal Importance	Q1 Count	Q1 Percentage	Q2 Count	Q2 Percentage
1 unimportant societal goal	44	5.3%	165	20.0%
2 minor goal	40	4.8%	164	19.8%
3 moderate goal	104	12.6%	232	28.1%
4 important goal	187	22.6%	178	21.5%
5 highly important societal goal	451	54.6%	88	10.6%
Total	826	827		
Mean	4.16	2.83		

Table 3.1 - Government Privacy (Bethell 2002)

(Bethell 2002) also conducted a similar survey to better understand societal behavior based on privacy concerns in the commercial sector. It asked the following questions regarding commercial sector privacy:

- Questions 3) Information contained in commercial data sets about the locations of an individual's activities should be kept private.*

Question 4) Private companies should be allowed to exchange information about the locations of an individual's activities to accomplish commercial objectives.

Table 3.2 indicates that most people consider privacy to be a highly important societal goal with regard to the commercial sector. The percentages are very high in terms of data in commercial databases being kept private. Although they are considerably less in terms of question 2 being a highly important societal goal.

Societal Importance	Q3 Count	Q3 Percentage	Q4 Count	Q4 Percentage
1 unimportant societal goal	36	4.3%	459	56.0%
2 minor goal	36	4.3%	173	21.1%
3 moderate goal	105	12.5%	121	14.8%
4 important goal	205	24.4%	45	5.5%
5 highly important societal goal	458	54.5%	22	2.7%
Total	840	820		
Mean	4.21	1.78		

Table 3.2 - Commercial Privacy (Bethell 2002)

The federal government is required through FOIA to allow public access to most of the data it collects and some government agencies are making their data available over the Internet in an attempt to minimize the amount of work required to fulfill information requests (Onsrud, Johnson et al. 1994). Having personal information records available online is disconcerting to many individuals and the public is beginning to question the effectiveness of existing privacy laws (Onsrud, Johnson et al. 1994). Many people do not realize how easy it is for companies to cross reference information about them. They feel that since they do not give out their social security number it is difficult to identify them

individually but every time they fill out an application they include an address (Bethell 2002).

Companies also have access to a variety of data, which allows them to better target potential customers or to better serve current customers. Spatial technologies have the ability to combine large amounts of data into meaningful profiles that can allow potentially intrusive access to a person's private information. In fact one of the most frequently raised concerns in the development of geographic information technologies is this simplicity in the integration and structuring of large amounts of data. Companies aggregate information such as census data, home prices, and purchasing histories to make studies of a household's shopping preferences. A common goal is to amass as much information about customers as possible in order to create profiles and offer personalized services with items they are most likely to demand (Curry 1995). This chapter sets forth a general discussion on privacy as well as its relevance in location technologies.

3.2 Privacy and LBS Environments

The previous section set the background for the privacy issue; this section relates privacy specifically to location service environments. In one example that is more specific to location technologies "the LBS industry took out an advertisement where a shopper received a coupon for fifty cents off a double non-fat latte on his mobile device while walking by that gourmet coffee shop - to show how relevant location-based advertising could be. Privacy-industry representatives used the same example to show how intrusive it could be. Most of us would prefer location-based services on our own terms: when I need it, tell me what's near me or near where I'm going. The problem with

typical location-based services is that they provide services about where you are” (Gutzman 2001). We can see from the examples illustrated below that some measure of privacy is essential for our personal safety and security.

3.2.1 Assessment of Privacy Risks in LBS

The following is an illustrative example used to explain the privacy problem with regard to emerging spatial technologies. In 1996, Beverly Dennis sued a company called Metromail because they used prisoners to compile data on individuals and one of those prisoners began harassing her. She found the Metromail had twenty-five pages of information on her including her income, preferences for soap and magazines, and even when she used hemorrhoid medicine. Dennis felt that her privacy had been severely violated. Metromail can no longer use prisoners to process their data. When prison officials lost the revenue from data processing they moved to creating maps with GIS (Bethell 2002). Another application allowed users to access tax information about every home, photographs of the residence, and consumer profiles. And although there were no prisoners gaining access to the records in this case, many found the situation dangerously alarming (Sykes 1999).

Location information generated in LBS environments can have major privacy implications, especially when we deal with the location information of individuals. It is necessary to consider their personal information privacy as a very sensitive issue. Massive quantities of location data are produced in LBS environments and are available and commonly used by combining data from many sources with the help of other technologies such as GIS and GPS. Many feel that privacy becomes threatened with the

ability to combine geographic information with personal information through a GIS and location technologies (Dobson 1998). Privacy works on the principle that people will select the data about themselves they wish to make public. It also relies on people forgetting some things allowing for the possibility of redemption (Curry 1995). Some theories present the idea that constant surveillance and the fear of punishment for transgressions will alter a person's behavior (Whitaker 1999).

With the advent of high bandwidth wireless networks more and more people are subscribing to location-based services in order to obtain geographically based information concerning various facilities and activities. "The data from these inventorying and tracking systems are being made pervasively available for commercial, government, educational, scientific and non-profit purposes. The further commercialization and availability in the private sector of adaptive orientation, smart identification, insitu modeling and similar intelligent spatial technologies significantly increases the already heightened location information privacy concerns of citizens" (Onsrud 2001). Numerous recent studies indicate high levels of consumer concern about threats to their personal privacy and a recent report of the U.S. Senate Judiciary Committee emphasizes that the expansion of e-commerce may be jeopardized if consumer concerns are not addressed (U.S. Senate Judiciary Committee 2002) As a consequence of the current amassing of data by location combined with the potential for detailing the mobile activities of large segments of the population, exposure to potential misuse of location information about individuals is substantial. In some instances, such as in a personal emergency or in a military operation, the external visibility of location information may be very beneficial to the individual. In other instances, external

surveillance may be a severe intrusion violating basic rights of freedom assumed by individuals in democratic societies. In order to improve the adaptability of these new technologies, privacy concerns need to be accounted for from the outset in the design and coding of intelligent spatial technologies. The Federal Trade Commission treats security as one of four primary elements that need to be addressed by government and corporate “fair information practices” in order to protect the privacy of individuals (FTC 1999). Privacy concerns typically arise when personally identifiable information is collected without the consent or knowledge of the data subject and made available to others without his or her consent or knowledge. Security breaches typically involve access to information or the interception of communication by unauthorized third parties.

The ability of the location-based service provider to collect location data brings the above mentioned privacy concerns to the forefront of many discussions. These concerns may ultimately prevent us from achieving the broad range of benefits that otherwise would be available to consumers (Onsrud 2001). The information amassed gives service providers the ability to engage in transactions concerning the dissemination of a user’s location information to third parties for financial gain. In most cases such activities are unknown to the user. This leaves subscribers in the vulnerable position of not having control of their own location information.

The rapid rate of development of location tracking devices gives way to a variety of highly intrusive applications (Clarke 1999). These technologies present the risk of monitoring individuals’ behavior patterns. GPS (global position systems) are being placed in more and more technologies. Cell phones contain GPS so that calls to 911 can be traced to a location. Systems are being created so the cell phones can be continuously

tracked while the phone is on. Cell phone tracking offers businesses the opportunity to distribute advertisements over cell phones to people as they walk past a business (Hoofnagle 2002). Cars contain GPS in order to accurately track the location of any vehicle and to assist the driver with navigation instructions. Whenever a GPS is turned on it collects information on the position of the unit. When an individual carries around a GPS, others can know where that individual is and sometimes what they are doing. A recent case involving a car rental company shows that GPS can be used for more than what the user intended. James T. Fleming rented a car from Acme Car Rental that contained a GPS system. The contract stated that if the driver exceeds the speed limit he or she could be fined \$150. The car company determined from the GPS unit that the driver went over the speed limit 3 times. The company withdrew \$450 from his account before he even returned the car. In the end the Connecticut Department of Consumer Protection ruled this was in violation of state law (Hoofnagle 2002). This case and others illustrate the potential of geographic technologies for personal privacy. Societies place limits on the amount of privacy invasion they are willing to permit (Clarke 1999). Efforts should be made to determine how to protect individual privacy in geographic information systems so these limits are not exceeded.

Companies have become increasingly dependent on customer information in order to make knowledgeable decisions and many resort to offering discounts and benefits through programs such as frequent buyer cards (Clarke 1999). On the other hand individuals are becoming increasingly wary of providing information to companies, especially when it comes to their past, current and future locations. They find it highly alarming and intrusive that their location histories can be mapped out over periods of

time. A standard is being set where individuals must determine how much their privacy is worth and who they are willing to sell it to. However, as mentioned before, previous methods have used a minimum standard approach that does not work for everybody. It has commonly been referred to as a “one size fits all” approach (Onsrud 2001). Once an individual provides information to a company there is little they can do to prevent the transfer of information to other parties. Thus this static method needs to be overcome by a more dynamic approach. The next section uses examples to demonstrate the extent of the privacy problem in location-based services and how they are being dealt with through traditional minimum standard approaches. It analyzes the benefits and shortcomings of such methods.

3.3 Prior Approaches for Privacy Protection in LBS

Most companies, government organizations and consumer groups recognize the widespread concerns about privacy and unsolicited wireless advertising in the adoption of LBS. The Cellular Telecommunications and Internet Association (CTIA) asked the FCC to create specific rules about wireless location privacy. The CTIA proposal says a technical solution must include notice, consent, and security and be technology-neutral (TechTarget 2001). As described in previous chapters, the current pursuit by others is towards minimum standards approaches. Policy based approaches have been researched from many angles and still continue to be the major player in resolving privacy in LBS. This section outlines the approaches taken by the following:

The Platform for Privacy Preferences,

The Internet Engineering Task Force (IETF) Geoprivacy Requirements, and the
Location Interoperability Forum (LIF) Privacy Guidelines

3.3.1 Platform for Privacy Preferences

“The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, it enables users to understand and most importantly act on what they see” (P3P 2003). P3P is a somewhat dynamic method implemented on the web. It is one of the major motivations behind the proposed “User Controlled Location Privacy Model”. According to Roger Clarke “P3P is a brave attempt to establish a technological basis whereby trust can be developed between pairs of consumers and marketers. A number of causes for concern exist, whose resolution depends in part on the web-community, but in part on law-makers” (Clarke 1999). An outline of the positive aspects of P3P is as follows:

- Relatively simple, easily understood, and easily implemented
- Integral to WWW technology, especially XML/RDF
- Reasonably sophisticated and moderately broad in scope
- Reasonably flexible, extensible and imminent (Clarke 1999).

He contends that there need to be political motivations, and economic incentives and disincentives, sufficient to energize Internet technology providers, web-site providers and web-users. In short, P3P has been invented; but for it to become an innovation, an adoption process has to occur. P3P creates the possibility for users to bring pressure to bear on web-site providers to express acceptable practices. The concerns expressed above about P3P's coverage are one cause for skepticism. Doubts about whether web site providers will actually deliver against their practice statements is still to be seen (Clarke 98). In any case P3P is a highly active program that is garnering a fair bit of attention. Hundreds of websites are now P3P enabled and it is gaining popularity (P3P 2003). However, its ultimate success is still to be seen. The dynamic contractual environment is somewhat similar to the Platform for Privacy Preferences in a theoretical concept sense, as it also provides users with modifiable privacy preferences that can be changed on an ongoing basis. However, the details and logistics are applied from a location privacy perspective as opposed to an Internet Privacy perspective. This changes most of the parameters from a general Internet environment to a more specific mobile tracking scene where the mobile device's privacy preferences are modifiable in a dynamic manner.

3.3.2 The IETF Geo Privacy Internet Draft

This initiative considers Location-based services (LBS) and other location-dependent services and the geographic location information about a mobile device (user, resource or other entity). It recognizes the fact that the information generated in the process of this emerging LBS model has major privacy implications. The IETF Geo Privacy group is pursuing the development of a set of industry wide protocols that might

help resolve privacy issues in location service environments (Cuellar 2002). The Internet draft assumes only the current state of readily available technology rather than development of new technologies and techniques to aid in the protection of privacy. It describes the requirements for a geo privacy protocol with intended use for the transfer of location data between primarily the user and those in the chain of providing location-based services. It focuses on authorization, integrity and privacy in LBS environments. The purpose of the geo privacy protocol is to allow policy-controlled disclosure of location information for location-based services. The person or entity with control over the policy and thus the level of privacy protection is defined as the “owners of the privacy rights of the target” (Cuellar 2002). Presumably this entity may in fact be one of numerous potential parties depending on corporate decision-making in the development or operation of a service. Among others, the owner could of course be designated as the owner of the mobile device being tracked but this is not expected to be the usual owner designated by industry.

The draft focuses on user-controlled policies. These describe the permissions (or consent) given by users of location-based services. The policies specify the necessary conditions that allow a location-based service provider to forward this location information. The user is able to specify which component or derived measure of the information is to be released to whom and in which granularity or accuracy. However, the draft does not suggest any minimum privacy levels or policies at this time. It also fails to elaborate on the various implementation options that will be pursued by competing LBS providers in order to address privacy concerns over the control of the location information. In addition to the above, the geo privacy protocol stresses security to

guarantee the correctness (integrity) and the confidentiality of the location information. This includes authenticating the main entities involved in the protocol and securing the exchanged messages. It discusses several particulars about the exchange of location information based on a privacy policy approach. Some examples of policies as described in the draft are shown below (Cuellar 2002).

- o "My family is allowed to know my street address; Yes No*
- o within 8am-5pm during working days my boss is allowed to know the city and*
- . if I am inside a campus of my corporation, then also the campus, building, and room number;*
- o any member of my corporation is allowed to know the time zone I am."*

Some of the service scenarios suggested by the draft are:

"Here I am!" Services

After locating himself, the target (=owner) may send his location to the Ultimate Location Recipient. In this service, the target (=owner) may take the initiative to send the location, rather than responding to requests.

"Where am I?" Services

These are services where the Location Recipient wants to know where he is, but he does not have any Location Data resources needed.

"Where is he?" Services

Location Recipient wants to know where a given target is.

Hence, the draft does describe the above scenarios with certain examples, and it is possible to get a sense of how things might work. However, more clear and consistent explanations of the protocols and a simpler model might be necessary.

The draft is a step in the right direction, but it is far from being a comprehensive solution to the problem at hand. It makes many valid suggestions such as, whenever possible the location information should not be linked to the real identity of the user. It also considers the possibility of the user hiding the real identities of himself and his partners not only to eavesdroppers but also to other entities participating in the protocol. The draft presents an interesting approach with several benefits. However, a major concern is that the model is somewhat static in nature and the imposed policies can only be changed upon an explicit update request by the LBS user. It is also a solution proposed largely by companies involved in location-based services. The draft is unclear in regard to numerous issues and therefore subject to broad interpretation by the industry who are likely to interpret any ambiguities in their favor over the interests of users (Onsrud 2002). It makes a number of points and contains some useful solutions. However, it is an Internet Draft and it has a long way to go before it can be developed in a useful and implementable technology.

3.3.3 Overview of LIF Privacy Guidelines

The world's three largest mobile phone manufacturers Ericsson, Motorola and Nokia founded the *Location Interoperability Forum (LIF)* in October 2000 to achieve the goal of offering location-based services worldwide on wireless networks and terminals (LIF 2002). This detailed document outlines the guidelines of the Location

Interoperability Forum for location data privacy. The target audience is application service providers, application developers, operators, terminal and network infrastructure manufacturers and other parties involved in the Mobile Location Service industry. The Guidelines are used in the LIF specification work and have been contributed to relevant standardisation bodies. These guidelines are based on the fair information principles of the OECD, regulatory requirements, active or emerging, and expected demand from customers. The guidelines are intended to help anyone developing or providing Mobile Location Services to better comply with privacy. The LIF Privacy guidelines represent a recommendation, not a standard or regulation. Therefore, compliance to these guidelines is not mandatory for any party although many companies are starting to contribute and use these standards. This section details this initiative and outlines benefits and shortcomings of LIF's Privacy Guidelines.

3.3.3.1 Definitions

By introduction the following definitions are drawn from the LIF Privacy Guidelines (Oinonen et al 2002).

Aggregate data - Data that is separated from all personally identifiable information.

Consent - Agreement to collection and disclosure of location data under specified circumstances.

Controller - The person or juridical person who controls the privacy preferences.

The Controller is normally the same as the Subscriber.

Informed consent - Consent that is given, with the opportunity of being informed of the consequence(s). Consent means permission to give location data to a requesting party in this document.

Location data - Geographical position of the target at a given time (lat/long/elevation or in another format)

LCS client - A location based service that requests location from a location service (LCS).

Personally identifiable information - Information that can be used to identify a physical or juridical person.

Requestor - The originating entity that has requested the location of the target.

Subscriber - A subscriber is an entity (e.g. a user or juridical person) that is engaged in a subscription with a service provider. (The subscriber pays the bill of the subscription and may be the employer of the target.)

Subscription - A subscription describes the commercial relationship between the subscriber and the service provider.

Target - The entity being positioned. It can be a person, an animal or a vehicle, for example.

3.3.3.2 LIF Privacy Model

Without going into too much detail about the conceptual architecture, it is important to pay attention to their language concerned with the disclosure of location data. Their basic principle for disclosing location data is confirmed opt-in, which means that the controller must give his/her informed consent for collection and disclosure of

location data (Oinonen et al 2002). The controller shall know the purpose of the collection and to whom it is disclosed for the opt-in to be informed (Oinonen et al 2002). “A target terminal offers two other functions related to privacy in addition to the access to an application: notification with or without confirmation. Notification informs the target about ongoing positioning and confirmation means asking permission for positioning. The use of notification and confirmation is a part of the rules database configuration” (Oinonen et al 2002). Reasonable security safeguards according to Federal Information Privacy guidelines are used to protect a disclosure (Oinonen et al 2002). “To achieve this authentication of the LCS client, encryption of the data will usually be required. If the application is inside a trusted domain, such as operator premises, and only trusted parties can use it, authentication is not mandatory. It is important that all the third parties to whom the location data is disclosed know how it may be used. Therefore the policies agreed between the location service and the controller party must be disclosed together with the location data” (Oinonen et al 2002).

There are two ways of getting the controllers informed consent for collection and disclosure of location data:

“***Permission asked*** - The authenticated identity of the requesting party is presented in an understandable form to the controller. Additional information like the planned usage, policy on storage and forwarding to third parties and if anonymity is offered may also be given. The now informed controller decides whether location data may be collected and disclosed in this specific case. The controller may optionally give permission for a longer period or even permanently” (Oinonen et al 2002).

“Predefined permission - The controller has beforehand given informed consent for one or several location services. Special care should be taken with written or electronic subscriber agreements where privacy preferences are given together with other service subscriptions. Changing of user preferences must be easy and free of any additional charges” (Oinonen et al 2002).

The controller may accept disclosure of location data under anonymity and the identity of the target is not known by the location service as it is translated into a temporary pseudo identity. In this way the target remains unknown for the location service. “If the same temporary identity is used over several requests, i.e. to build up user preferences, the anonym becomes a pseudonym. This could happen through one time or predefined permission and in both cases anonymity is recommended” (Oinonen et al 2002). The guidelines suggest that personally identifiable information should only be made available to service providers when it is required to provide the value added services and special care should be taken in order to ensure that anonymous location data cannot be connected to an individual (Oinonen et al 2002). Another key element to protect anonymity is to make sure that the disclosed location is not more accurate than necessary for the service. Also “the location data should not be stored except where necessary for the provision of the service and subject to user's informed, unambiguous consent. (i.e. there should not be any sort of ‘log’ of the location of a target)” (Oinonen et al 2002). The quality or type of disclosed location data can be modified or degraded before disclosure to improve privacy. For example, if accuracy is at a course-grained level, such as a city instead of a street, this might be an acceptable level of privacy for some users or use cases. The general rule is that the disclosed location data should be of as low accuracy as possible

for the particular application (Oinonen et al 2002). Location data is only provided when a specified purpose of usage is given and an important issue is also whether location may be given to a third party, and under what conditions. The controller might also want to limit the length of time that the location data may be used by the other party. These preferences have either been configured by the controller and are delivered to the application together with the location data, or the application has presented a policy as to how to handle location data and the user has decided to accept that policy (Oinonen et al 2002). A key issue is that all the players in mobile location services value chain have the same understanding of privacy and practices that don't leave any holes. "If disclosure procedure, for example, is handled properly, but location data ends up in the hands of a third party, which does not respect the agreement on policies, privacy is lost. Privacy requires chain of trust, which is based on agreements. The trust chain begins from the target terminal, goes through an operator and service platform, and through one or more service providers" (Oinonen et al 2002).

The above initiatives are currently in place to promote personal information privacy. None of the approaches have been implemented on a wide scale, but each has its own set of supporters and opponents. These in no way represent all the research being conducted, but they are some of the more important works at this current time.

CHAPTER 4

USER CONTROLLED PRIVACY PROTECTION IN LBS

4.1 Introduction

Our hypothesis is that *it is possible to develop an approach for protecting privacy in the use of location-based services that supports the core ethical principle of autonomy of the individual*. This hypothesis is tested, not by providing an operational system, but by developing a combined legal and technological *conceptual model* that places the power to protect location privacy in the hands of consumers of location-based services (Onsrud 2003). The contract-based model addresses issues such as who controls the location information, how accurately should service providers be allowed to track moving objects, what data retention times are acceptable, what an entity in the process can do with location information and several other areas of concern. We will try to address the cost of such a model, keeping in mind that we need to consider the technological cost of communication and computational operations as well as the monetary costs behind implementing such a ground-up system (Bhaduri and Onsrud 2002).

Location prediction and the querying of moving objects are important topics that challenge the practical applicability of the proposed model (Sistla, Wolfson et al 1997). The monetary cost of changing contracts on an ongoing basis is something that would also require a great deal of attention. A major goal of this thesis is to create an operational vision supporting user controlled protection of privacy that can help direct technological efforts along appropriate paths.

4.2 User Controlled Privacy Protection Model

Initiatives such as the Platform for Privacy Preferences suggest an initial conceptual approach for addressing personal information privacy protection for location-based services. Although not yet fully functional, the approach will enable web sites to automatically inform users of any web site's consistency with preset privacy preferences of the user (P3P 2002). If inconsistent, the user has the option of changing preferences for the specific application desired in order to gain the benefits of that application. The individual user also has the ability to disengage from personal data collection when an application is no longer desired (P3P 2002). In a similar manner, location based services should use a standard method for declaring personal information and location information needed or desired for specific applications and provide a system upon which users may depend to respect their privacy preference choices (Onsrud 2001).

4.2.1 Definitions and Architecture of the Approach

The following simplified terms are used throughout the remainder of this chapter. The definitions extend from those proposed in the IETF Internet Draft (Cuellar 2002) and differ somewhat from the definitions as used in the LIF Privacy Guidelines of Chapter 3 (Oinonen et al 2002).

Target - a mobile electronic device that may be tracked by location

User - person associated with a specific target

Server - an entity that knows about a target in terms of identity, location, and time of location

Client - an entity that wants to know what the server knows, typically for some business purpose. In other words a third party.

Figure 4.1 illustrates the basic architecture of “user controlled privacy protection in LBS”. It shows the flow of data between the parties defined above and a layer between the “User” and the “Server”, where the user has the ability control privacy preferences.

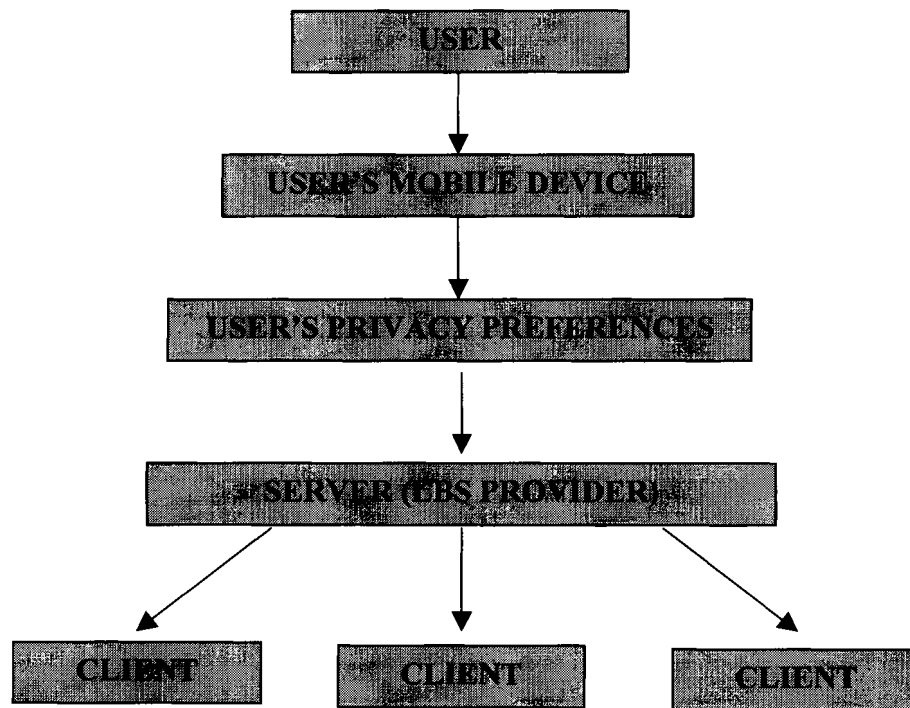


Figure 4.1 – Architecture of the “User Controlled Privacy Model”

4.2.2 Functions of the “Personal Communicator”

Although a **target** may take many forms and be labeled as a phone, personal digital assistant, laptop or GPS unit, the term in this chapter used to generically describe all such electronic devices and synonymous with "target" is "personal communicator" (Onsrud 2001). This thesis uses the "personal communicator" as an example for the “user controlled privacy protection model” and the model will be demonstrated in terms of this

device. Figure 4.2 illustrates the main menu of the “personal communicator” in the mock-up prototype. This screen shows a number of functions such as phone, e-mail, web, other services and settings privacy preferences. The focus for this thesis is the “setting privacy preferences” function, which leads users to a list of privacy preferences that can be individually modified as per a particular user’s needs. At the bottom of the device the left arrow takes the user to the previous screen and the right arrow takes the user to the next screen. The center globe button can be used to return to this main menu. The e-mail, web and other services buttons are place-holders and are not described in this thesis, as they are merely examples of options in a typical LBS interface and do not necessarily factor in to the privacy discussion at this time. The “off” button is used to shut off the “personal communicator”. The importance of this option will be apparent in section 4.2.5.1.

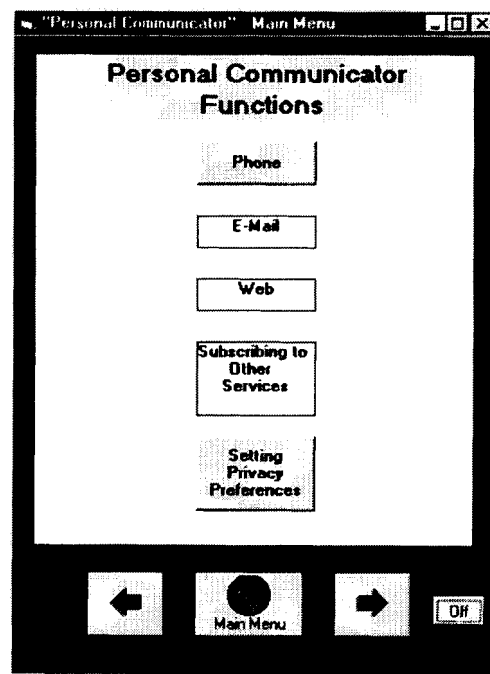


Figure 4.2 – The Personal Communicators Main Menu

Note that a **user** and **target** are typically treated as one and the same by the server and client. However, differentiating between the terms helps highlight that a target (i.e. the device) may be left on a bus and follow a very different path from that of the associated user. Automated fingerprint and similar identification techniques might, of course, be used to provide more secure evidence of when the user and target are together, though those lead us into more pervasive and ubiquitous computing environments that are not an area of concern for this particular project. A typical **server** would be a telecommunications carrier engaged in providing wireless location services. The **client** is thought of as a client of the server rather than a client of the user. A typical **client** might be an existing business that wants to sell a product or a service to the user. By example, the client might want to engage the user in commerce through (1) a real-world transaction (buy your favorite brand of jeans in your size at 20% discount at the store right in front of you), (2) virtual-world transaction (your favorite band is playing a concert at 7:00 p.m. in the city in which you just arrived - buy an electronic ticket now), or (3) provision of an on-line service (five of your friends are within 500 feet of your location and want to meet you at the next street corner - see map) (Onsrud 2001).

As the wireless location industry grows, the distinctions between **servers** and **clients** may become very blurred (Onsrud 2001). Servers are likely to want to provide many products and services directly rather than go through other businesses. Figure 4.3 shows how a phone menu could be designed in the “personal communicator”. The phone can have its own set of settings that can be modified by the user. In terms of privacy preferences for phone calls, they are addressed individually for each particular setting in the privacy preferences menu.

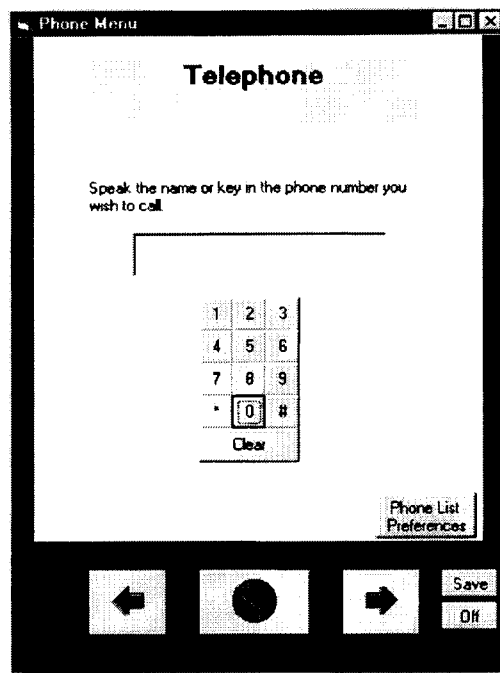


Figure 4.3 – An Example of a Phone in the Personal Communicator

4.2.3 A Model Contract Approach for Location Privacy in LBS

Model contract language can help provide consistency in achieving goals across an entire industry. While a specific contract approach among network service providers (servers), application developers (clients), and users can't be forced upon an industry; certainly a range of incentives may be used to encourage consistent yet flexible approaches for the protection of personal information privacy. For instance, government may use adherence to a model contract with consumers as a precondition to granting of permits or to participation in tax incentive or funding programs. Government funding also might be used to create open source code that would provide for the automated enabling and enforcement of model contract provisions. Such code would be made available for use by all in the industry (Onsrud 2001).

Some of the language that might be included in such a model contract follows:

The following preference settings established by <name of **user**> are understood to constitute an enforceable contract and are binding among all parties engaged in providing location-based services to the user, including but not limited to <name of server>, henceforth known as **server**, and all **clients of server**. The terms of this contract may be changed at will and without notice by the user through the altering of the following preference settings. The altering of preference settings by the user automatically changes the terms of this contract in accordance with the changed settings. The server and all clients of server agree to responsibly adhere to and enforce all current and future preferences stipulated by the user. Adherence and enforcement is expected to be implemented primarily through code and thus automatically upon request by the user.

Preference settings have been preset to maximize the potential utility of current and future location based services for the user. Users are responsible for changing preference settings in order to gain higher or lower degrees of personal information privacy protection over the time of their relationship with the server and clients of server (Onsrud 2001).

4.2.4 Settings of the “Personal Communicator”

Under the envisioned approach the user would specify separate preferences for the following categories of entities or individuals with whom the user might want to communicate.

1. Off Condition Privacy Preferences

2. Emergency Response Privacy Preferences
3. Communication List Privacy Preferences
4. Clients of Server Privacy Preferences
5. User as Consumer
6. Server Privacy Preferences

Figure 4.4 illustrates the above options in the form of a menu in the “personal communicator”. This menu can be accessed by selecting the “setting privacy preferences” option that is shown in figure 4.2.

Each of the settings is individually described further in this section. The settings provide users with flexible options for providing themselves with as little or as much privacy protection as they desire. The settings are automatically enforced by computer code upon selection and transmission by the user.

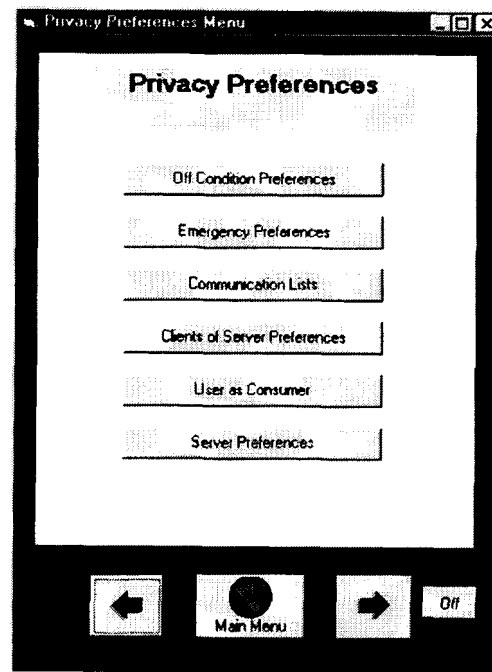


Figure 4.4 – Privacy Preferences Menu

4.2.5 Off Condition Privacy Preferences

Figure 4.5 illustrates the “Off Condition Privacy Preferences”, which mandate the user’s preferences when the device is turned off. Assuming that the location fixing technology works independently from software on the device, the server may be able to track the “personal communicator” even when it is turned off. Hence, the user is given the option to decide the level of tracking he or she desires. This option can be changed at any time by accessing this preference from the preferences menu. This could also be an essential component for emergency situations. By example, a user selecting the second option could turn off the mobile device, but still be located in case of an emergency.

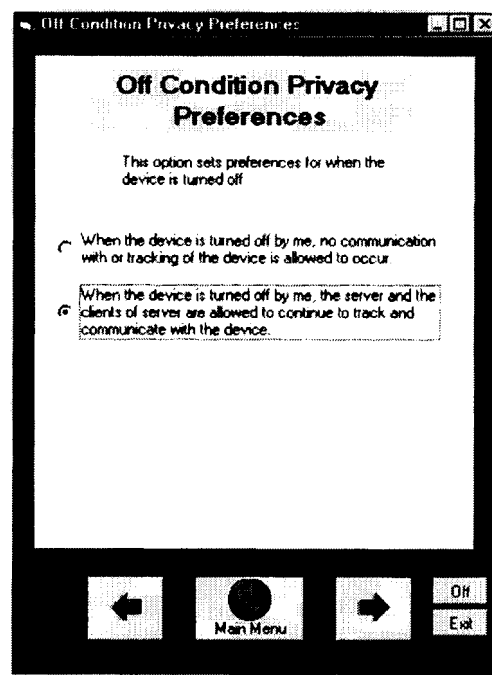


Figure 4.5 – Off Condition Privacy Preference

4.2.6 Emergency Response Preferences

Calls by the user to 911 and to additional emergency phone numbers specified by the user override all other preferences. In the event of an emergency call by the user, the user may be located as accurately as possible and emergency responders may communicate with the user through the device by any and all means available.

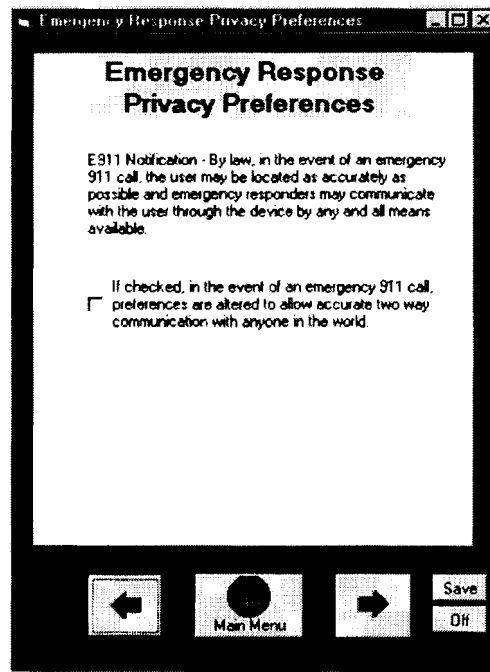


Figure 4.6 – Emergency Response Preferences

Figure 4.6 shows the E-911 notification. If the box has been previously checked, the communicator reverts to a phone with no restrictions in an emergency allowing anyone in the world to get through to the user.

4.2.7 User Specified Communication List Privacy Preferences

This preference helps the user construct and maintain communication lists and apply different privacy preferences for each one. Figure 4.7 illustrates the index menu for

establishing different lists. A user can create a list such as “Business Associates” by selecting the button titled “Create Another List”. Once created the user places individuals on the list by selecting “List” and sets privacy preferences by selecting “Preferences”. Each list can be activated or deactivated at any given time. By example, if a user is on vacation and does not want to be contacted by business associates, then he/she can just uncheck the “Business Associates” option and business associates will not be able to communicate with the users “personal communicator”. On the other hand, if the user is at work, he/she can choose to uncheck the “Friends” list and so on. If the option “Anyone in the World” is selected the communicator operates much like an open phone but with privacy limitations discussed in section 4.2.8.3.

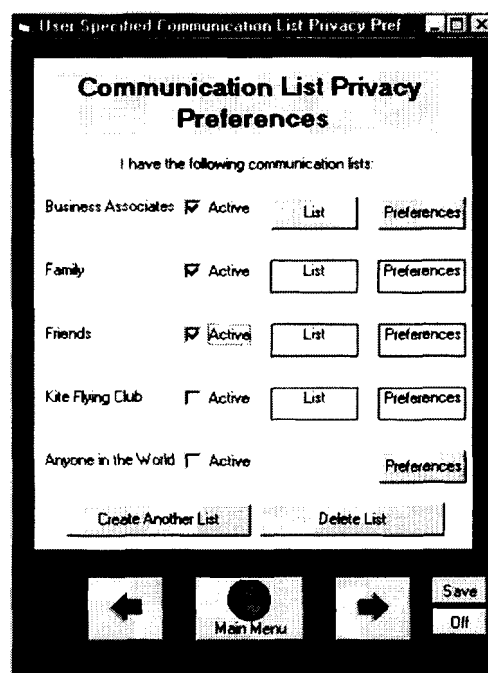


Figure 4.7 - Communication List Privacy Preferences

4.2.7.1 User Specified Lists

If we click on the “List” button next to “Business Associates” in Figure 4.7, the device brings up the names address and e-mail addresses of the people included in that list. A user can create a new list or delete an existing list as and when needed. Figure 4.8 shows the “List of Business Associates” that includes the names, addresses and e-mail addresses of business associates. If the communicator is set to allow incoming communications only from “Business Associates” the device checks to see if there is a match with the incoming phone number, e-mail address and perhaps name. In the example if the incoming call came from (207) 866-1345, the call would be allowed through. A user can toggle through the contacts alphabetically and also add and delete contacts as necessary in a specific list. Other lists can be handled in similar fashion.

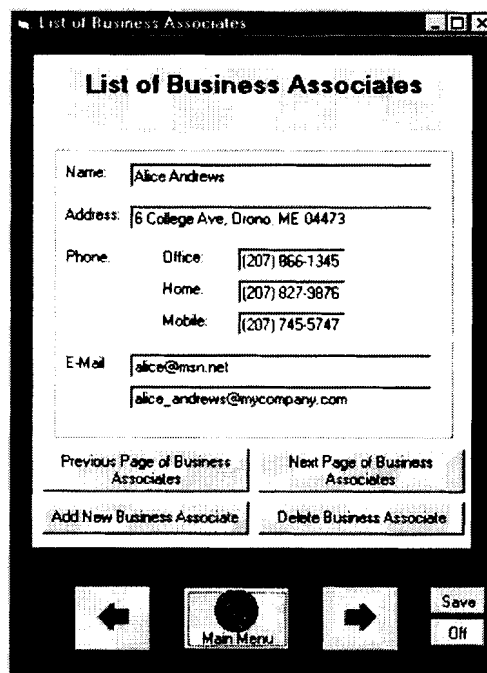


Figure 4.8 – List of Business Associates

4.2.7.2 Privacy Preferences for List of Business Associates

The privacy preferences associated with a list are illustrated in Figure 4.9. A user can specify if the “personal communicator” can or cannot receive phone calls, text messages and others items from business associates. One of the other key features of the model that provides additional flexibility is the option to select how others may view a users location data. As shown, the user may specify the accuracy to which the user will allow a list of people to track the device in time and space.

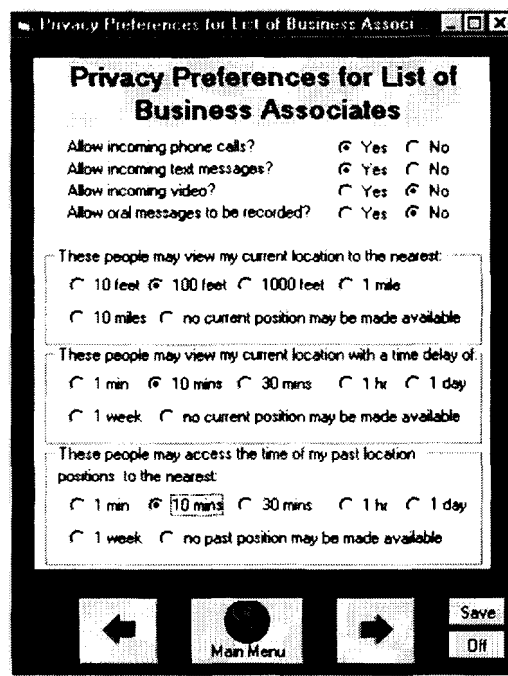


Figure 4.9 – Privacy Preferences for List of Business Associates

In Figure 4.9, the user chooses to allow incoming phone calls and text messages from business associates, but selects “no” for the other options. Additionally, the user allows business associates to view her current location with an accuracy of about 100 feet, a time delay of 10 minutes and past locations may be pinpointed within only 10 minutes. Hence, the user is not restricted to a default set of preferences they may have agreed to when

they subscribed to the location-based service. Instead, the user has flexibility. The system acts as a dynamic contract that can be changed on the fly. This affords the user as much or as little privacy as they desire under different circumstances and over time.

4.2.7.3 Anyone in the World Privacy Preferences

The “Anyone in the World” option is also included in Figure 4.7. This option regulates privacy preferences for those callers that are not included in any of the users created lists. It operates similar to having a listed phone number. Anyone in the world who knows your phone number or e-mail will be allowed to communicate with you in accordance with the preferences when this list is activated. Figure 4.10 illustrates the “Anyone in the World” privacy preferences. In this example, the user allows the rest of the world to know where she is and when but not to the same level of accuracy as her business associates.

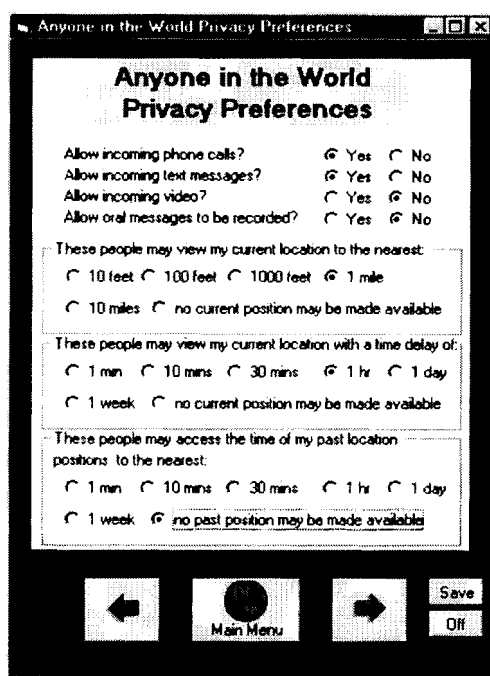


Figure 4.10 – Anyone in the World Privacy Preferences

4.2.8 Clients of Server Privacy Preferences

The fourth menu item in Figure 4.4 shows that the user also has the ability to control the level of access that clients of the server are allowed. Clients are typically businesses in the city in which the user is located that would like to make contact with the user when she is near their establishments in order to provide her with information she desires or possibly provide her with discounts. Other typical clients may be national and international virtual services that are able to provide you with on-line information, reservations and ordering of products wherever the user may be located.

Figure 4.11 illustrates how privacy preferences would function in the above case. The server (LBS service provider) gives the user the option to choose between pull and push marketing. If the user chooses to go with “Pull Services”, clients of the server may not know the user's location or only be provided the location when a user makes a specific request that requires the location. This means that the user maintains full privacy from third parties, except when their services are explicitly requested. On the other hand in “Push Services”, client businesses of the server may advertise and offer discount services. By example, if one selects this option for a certain period of time, they may automatically receive a 20% discount on the monthly LBS fee. This allows client businesses and servers to generate additional revenue and enables them to pass some of the benefits to the user. The tracking accuracy and timing delay options are the same as previously discussed.

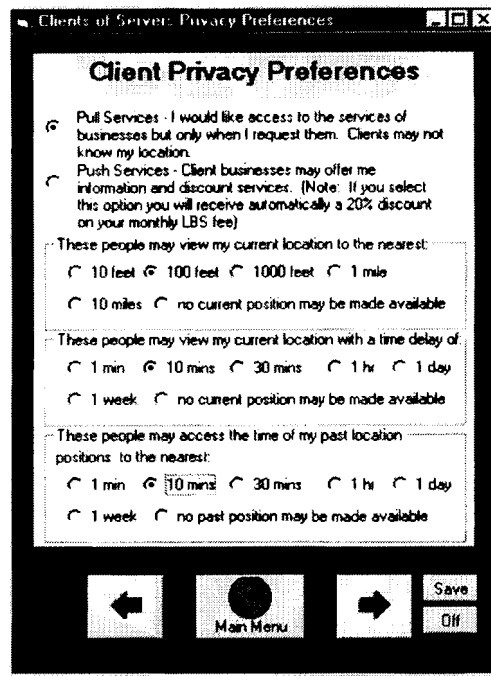


Figure 4.11 – Clients of Server Privacy Preferences

4.2.9 User as Consumer

The fifth menu item in Figure 4.3 illustrates that the user may want to specify specific products or services that the user is interested in pursuing as a consumer. In order that stores and businesses may offer products and services in which one may have a specific interest, users need to indicate their personal buying preferences. By supplying this information, stores may be able to offer discounts when they know that a user is near. Privacy preferences specified by the user should be rigorously enforced by computer code and may be changed at any time. Figure 4.12 illustrates how the “User as Consumer” interface might appear.

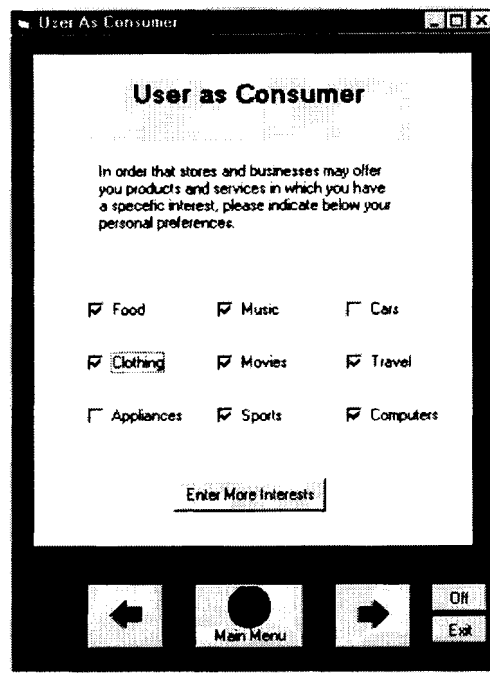


Figure 4.12 - User as Consumer Preference Menu

4.2.10 Server Privacy Preferences

The final menu item of Figure 4.4 is titled “Server Preferences”. The user’s privacy preferences regarding the server, meaning the LBS providers, are illustrated in Figure 4.13 and Figure 4.14. Figure 4.13 shows how accurately the server may track the device’s location and how long the server may retain the device’s past positions. An important feature to keep in mind is that the server needs to know a devices location, in order to provide services based on that location. Some scenarios regarding this situation are discussed further in this chapter.

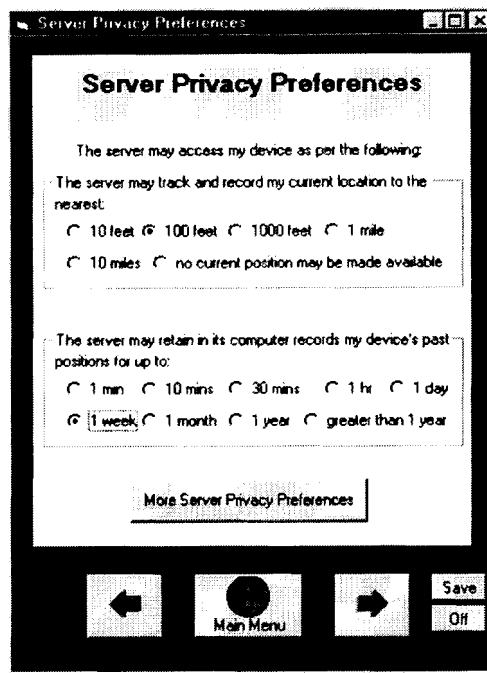


Figure 4.13 – Server Privacy Preferences

In Figure 4.13 we can see that the user has set preferences to allow the server to track locations up to a resolution of 100 feet and the server can store past locations for up to 1 week. By example, if the user currently prefers “push services” as described in section 4.2.9, the server may be able to store a week’s worth of location data along with consumer preferences and allow clients to advertise to the “personal communicator” based on the privacy preferences in the “clients of servers privacy preferences”.

Figure 4.14 illustrates some additional server privacy preferences, which can be accessed by clicking the “More Server Privacy Preferences” button in figure 4.13. These preferences describe how the server may sell or otherwise transfer current or past data collected from the “personal communicator” to third parties.

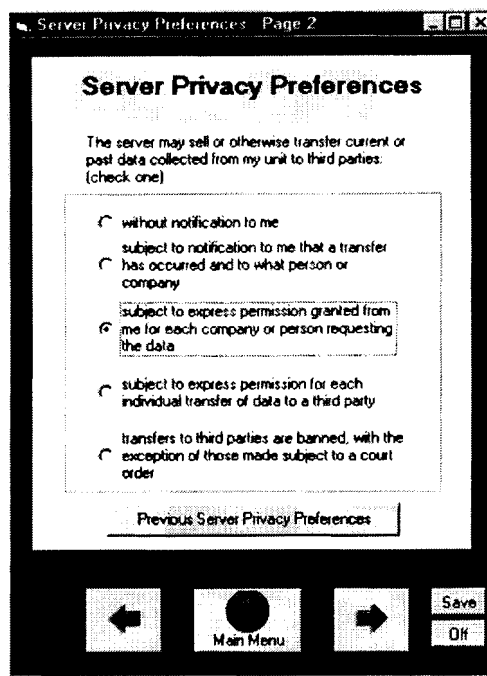


Figure 4.14 – Server Privacy Preferences (Page 2)

The example in figure 4.14 indicates that in this instance the user will allow the server to sell or transfer location related data of the personal communicator subject to expressed permission granted from the user for each company or person requesting the data. As mentioned previously, the user is informed if there are conflicts in changed levels of privacy. By example, if a certain user request requires the server to track the device with an accuracy of 10 feet, but the users privacy preference allows only 1000 feet, then the server should inform the user and ask permission before changing the setting to provide the requested service.

The server should also undertake the responsibility of protecting the users location information where needed. It should handle security with utmost diligence. A sample security notification made part of the contract obligation might be as follows:

Notifications from Server:

The Server acknowledges that data transfers from the user's personal communicator to the carrier <are><are not> encrypted.

The Server acknowledges that data received from the user's personal communicator <are><are not> stored and managed on a secure server.

All the above settings are of course built in and enforced through code. Modifications to preferences can be made as societal conventions and user desires change. The model outlined in this chapter illustrates the possibility of dynamic contract-based user controlled privacy protection in LBS in our future.

4.3 Conflicts in Privacy Preferences: An Operational Example

Servers need to know the location of a device, in order to provide services based on that location. However, consider the query, "Please locate all pharmacies within 500 feet of my location". In this case the servers' ability to track the device is set to 10 miles. Thus, the server cannot provide information with the required resolution of 500 feet if the server is not allowed to track the location of the device up to at least that resolution. To accommodate for such conflicts let us assume a user specifies a set of preferences on how she would like the privacy of her information handled by the server and any clients of the server. The user queries her personal communicator as follows:

"Please locate all pharmacies within 500 feet of my location."

The device might come back with a response such as:

In order to respond to this request your personal privacy preferences must be changed to the following settings:

Setting 6.1 - The server may record, display, and transmit my device's instantaneous position to the nearest 10 feet.

Do you agree to this settings change? Yes No

Should this change be incorporated in your default settings? Yes No

The example illustrates that users should be able to opt-in and opt-out of specific preference settings on the fly. The user can allow the server to change a server privacy preference to obtain a service and once the service is complete, the user has the option to keep the new server preferences or return to their previous preferences. Mobile location services that provide users with great flexibility and direct control over protecting their own personal information privacy are likely to grow quickly and become the most successful services in the marketplace.

4.4 Summary

To make money, the basic rule in business is to satisfy the customer or, in this instance, the user. There is no ideal level of privacy protection that will satisfy all users. In addition, a user's perception of how much privacy is desired and how it should be achieved is likely to change over time. Therefore, to satisfy all users all of the time, servers and clients need to transfer effective, efficient, and flexible control of privacy protection to users. By doing so, users are able to satisfy themselves with the level of information privacy they need in the use of location-based services. Those servers and

clients that achieve the goal of transferring privacy protection power into the hands of users are likely to gain enthusiastic participation in their location based services. This assumes, of course, that the services provide something of actual use to consumers. In addition, if consumers are provided powerful tools for protecting their own privacy but fail to use those tools, they will have only themselves to blame if a use they disapprove of conforms with the preferences that they themselves have set. Further, users will have the power to correct immediately the situation for their future use of location-based services (Onsrud 2001).

Companies that provide consumers with the ability to control their own personal information exposure will attract a huge customer base. In short, those servers and clients who are first to turn over control of privacy protection preferences to their users are the most likely to gain market lead in the mobile location industry and stay there (Onsrud 2001). The next chapter further analyzes the basic model presented above.

CHAPTER 5

FURTHER ANALYSIS OF THE MODEL

This chapter analyzes the model presented in Chapter 4. A quick recap of the contracting parties and the basic structure of the “user controlled privacy model is as follows:

- “Target” and “User” are the same in most cases, unless for some reason they are traveling separately.
- The “User” enters into a contract with the “Server”.
- The “Target” cannot enter into a contract as it is merely the device that is being tracked.
- The “Server” enters into contracts with “Clients”
- “Clients” are third parties and at the moment our model does not envision direct contracts between the “User” and “Client”. However, this could be a likely scenario in practice since the “server” and “client” might be the same in some instances. It is also possible to envision the “Client” directly contracting with the “User” although this is likely to result in greater inefficiencies in managing contractual conditions.
- Every time the “User” changes a privacy preference in the “target”, it is effectively a new contract. Typically our system allows for “Users” to use these dynamic contracts as per their needs at a particular point of time.

5.1 Key Questions

Chapter 1 presented several questions about a dynamic contract based user controlled privacy protection model such as:

What kinds of economic practices and pricing models will likely result from the proposed approach? Will the developed systems result in greater privacy protection for those who pay more? Is greater autonomy for each individual a morally appropriate design choice when in practice poorer people may have less choice than wealthy users? Will everyone in society in practice gravitate towards the lowest price and therefore the lowest privacy protection? When the user-defined contract allows the service provider to pass on location information about the user, should there be any limitations on the use by third parties beyond that proscribed by the legal system? For the ever-changing contractual relationships, how should the technology manage the status of the contract and the automatic enforcement of the contract provisions? Must an archival record be kept of all past user preference status conditions? What conditions will entice industry to adopt user-controlled dynamic privacy preference approaches?

Several of these questions are discussed in this chapter.

5.1.1 Pricing Model

What kind of pricing model would likely result from this approach? (Calling area, price based on time at a particular level of privacy, etc)

We envision and suggest for our model that the base price for providing personal communicator services should assume that there will be no third party users of the

information. When such use is allowed by a communicator user, the service provider is able to offer discounted prices in return for lower levels of privacy. In other words, if an individual is willing to forgo some privacy and open himself/herself to solicitations from the service providers or third parties, then they would pay a lower price for the service. The pricing model is uncertain until industry actually experiments with the approach. Ideally industry would like to keep prices at marketable levels, while providing the maximum amount of privacy that is possible at each level. Our vision is to make the billing and pricing procedures dynamic. Users should be able to switch through levels of privacy and be charged based on time at a certain level or the amount of marketing conducted at that level. Once users are accustomed to such a system and have reached a level of comfort with the amount of information they are divulging, it is probably inevitable that they will divulge increased amounts of location information in order to gain increased benefits or price reductions.

5.1.2 Putting a Monetary Price on Privacy

Will the developed systems result in greater privacy protection for those who pay more?

Our current model raises an important ethical question regarding the cost of privacy. Under such a model service providers are likely to offer discounted prices in return for lower levels of privacy. We don't see a major moral problem assuming that the minimum levels of privacy protection mandated by society through its laws are supported by the technology and as long as users have the option of changing their privacy preferences quickly and conveniently if they become uncomfortable with current levels of privacy being protected.

5.1.3 Moral Significance of the Model

Is greater autonomy for each individual a morally appropriate design choice when in practice poorer people may have less choice than wealthy users?

Until a market develops there is little to indicate that poorer people using such devices would choose to give up more information than wealthy people. Ownership of such devices, similar to the ownership of a phone, assumes that the user has sufficient wealth and desire to make use of the product. A poorer person might be more tempted to take advantage of price discounts but this is not necessarily so. By providing a single contractual model for all LBS servers a level playing field is created for all users, whether rich or poor. The system is designed to support “equal opportunity” but not necessarily “equality” in privacy protection. The “user controlled privacy protection model” in location-based services provides a simple tool for individuals to express their own autonomy.

5.1.4 Gravitation Towards Lower Prices

Will everyone in society in practice gravitate towards the lowest price and therefore the lowest privacy protection?

It is general human tendency to gravitate towards lower prices. Most individuals are able to rationalize and weigh tradeoffs between providing personal information and receiving monetary benefits. People generally try to obtain their money’s worth by going for the lowest prices and we expect this would be true in our model, at least through the initial stages when user adaptability is low. As users become more accustomed to the system, they will be better equipped to evaluate and decide their need for privacy and

how much value they place on giving up a certain portion of it or being subjected to unwanted solicitations. The dynamic nature of our model should be very helpful in this case. Users have the ability to try a certain level of information exposure and move up or down based on their needs at a certain point of time.

5.1.5 Archiving Preference Status

Must an archival record be kept of all past user preference status conditions?

This is important for the practical enforceability of the changing contract provisions. The history might be stored on the device or on a central server but recording in both locations would probably be advisable. Both histories should be identical and having the information stored in both locations would avoid the temptation for wide scale contract breaches against the user by the server.

5.1.6 Enticing the LBS Industry to Adopt Such a Model

What would entice industry to adopt such an approach?

The location-based service industry has no automatic intrinsic interest in pursuing a complex contract-based approach to protecting privacy in LBS environments. Industry has fairly short-term goals and it is customary to go with a solution that will yield maximum benefits in the shortest amount of time. Thus, in the case of privacy protection in location services, the industry has been pursuing a minimum standard approach. This approach minimizes the amount of control over location information that the industry has been willing to provide to the user.

The LBS market has grown much slower than originally predicted and we hypothesize that concerns over privacy are a significant impediment to growth of the market. Giving privacy control to users has substantial potential for creating the desired market and thereby the desired profits from such services. A dynamic technologically oriented system has potential to build the market.

It is important that external entities such as government and consumer groups encourage LBS companies to look into alternative approaches for location privacy protection. In order to get them to think along these lines, it is necessary to present a somewhat complete model that is technologically and conceptually sound. We believe that our research model is a positive step in this direction. Further development of our conceptual model would likely require further investment by the public prior to development investment by the private sector. This is due to a wide range of technological issues that yet need to be addressed, public goods aspects of the model, and the existence of vested interests in current private sector technological approaches. Alternatively, enlightened risk takers in the private industry might also pursue the approach. Consumer groups and privacy advocates have constantly pressured companies to improve location privacy. The LBS industry could play an important role by providing customers with comfortable levels of privacy and accommodating the interests of individuals or broad groups of users. For the most part, this is something they should want to do for their customers. The potential to attract customers, which is the primary market, should be the major driving force for industry. This may lead to short term revenue decreases in secondary areas such as the advertising market, but the benefits of attracting more customers should outweigh the cost of giving up control over location

information. A hypothetical example that could be used to explain how such an approach would work is illustrated in Table 5.1.

	Commercial Controlled Privacy Protection	User Controlled Privacy Protection
Fixed and Variable Costs	50	70
Subscription Revenue	100	250
Advertising Revenue	50	35
Total Revenue	100	215

Table 5.1 – A Hypothetical Cost Structure

In the above Table 5.1 we see that subscription revenues go up substantially and advertising revenues go down, but the total revenues go up. This is just a hypothetical situation, but it is important to note that the LBS industry has not grown as rapidly as originally predicted by analysts and is not because of a technological issue. In fact, social issues such as privacy need to at least be investigated to economically advance the industry.

5.2 Other Issues

Some miscellaneous issues related to the “user controlled privacy protection model are discussed in this sub section.

5.2.1 User Education

A careful evaluation of the conceptual model makes it quite clear that it is a fairly complex one. A formal implementation with further features might be even more

complex. It would be very important to engage typical potential users in all phases of designing the user interface as well as determining which location services users would actually make use of. If inappropriately designed a failed system would result. By example, it is possible that many users might never get beyond their preset privacy preference defaults. Hence, the system needs to focus on usability and provide the user with a simple interface that is not monotonous to use. As time progresses and users provide feedback to help improve the system, a much more efficient implementation would result. Another, quick solution could be setting default levels of privacy. By example the “personal communicator” could have an additional screen leading to the following preset preference levels.

“No Information”

“High”

“Medium”

“Low”

This user has the ability to see the specific settings at each level and thereby the ability to modify settings from then on, but this basic system could save a fair amount of time if a user can find the desired level of comfort within the predefined options. Thus, could users have detailed or general privacy preference tools.

5.2.2 Distributing Control over Data

The primary objective of our model is to provide the “user” with the ability to control their personal information and decide the level of privacy that suits them. It may be argued that not all customers can make this decision rationally but it is an individuals

democratic right to make their own calls. Users should have the right and ability to make mistakes. In our model the user is the owner of the data, but he or she can permit the “server” to use certain information for a specific purpose. The “server” can also try to obtain access privileges by offering the certain incentives. The “server” can provide or sell the data to “Clients” based on the “Users” authorizations. In all cases intentions should be made clear. If a user receives solicitations, it should be entirely by his or her choice. They have the ability to reduce or increase their own desired level of personal information privacy.

5.2.3 Technological Feasibility

Database Management Systems (DBMS) have been around for many years and they have become an essential element in the modeling of the world around us. Business, science and many other fields routinely use DBMS in various application domains. As technologies capture more and more of the infinite real world, the modeling has become extremely complex and cumbersome. Innovators that we are, we have met the challenge head on by continually developing new computerized modeling systems to pursue this never ending task. Existing database management systems have worked very well in the past and they are still more than sufficient to handle most of the data that might need to be modeled. However, “they are not well equipped to handle continuously changing data, such as the position of moving objects. The reason for this is that in databases, data is assumed to be constant unless it is explicitly modified”. Traditional DMBS deal with static data attributes at any given time. This has led to a rather discretely updated model.

In order to design systems that can address the dynamic nature of moving objects we need a continuously updated model (Sistla, Wolfson et al 1997).

To represent moving objects (e.g. cars) in a database, and answer queries about their positions, the positions of the object have to be continuously updated. But this is an extremely expensive operation in terms of the cost of computation and bandwidth. Hence we need to find alternative approaches to overcome this inherent problem. Ouri Wolfson and colleagues have provided one such approach, they suggest capturing the motion vectors (dynamic attributes of an object), such as speed and direction (Sistla, Wolfson et al 1997). Implementing these motion vectors into functional algorithms can provide us with the location of a moving object at any given point in time. They assume that the starting time (t) and the route for the moving object is known. For example, let us consider a car moving north at I-95 at a speed of 60 MPH. Assuming that nothing changes along this linear route, we can calculate the (X,Y) coordinates of the moving object at any given time t' given that $t' \geq t$. Depending upon the application domain, these motion vectors change a lot less often compared to the location coordinates of a moving object. An explicit update to the database is required only when there is a change in the motion function, which is made up of the dynamic attributes. This is one of the many feasible solutions to track moving objects in an efficient manner. Several others can track at certain intervals and interpolate between locations to come up with a pretty accurate location history. Technology is a major concern of this thesis and location-based services in general. Processor speed and bandwidth have already achieved incredible levels and they will continue to improve. The technology will evolve, but we need to have a robust conceptual framework to efficiently direct and utilize technological

advances. Hence research on combined social and technological in location environments is critical.

5.2.4 Security

When we consider the above scenario, it is imperative that security be addressed. If location information about a certain “user” is stored in a database, it must be protected. Service providers will need to maintain high levels of security to prevent interception of this information during communication or the acquisition of this information by non-authorized parties such as identity thieves, hackers and stalkers. The safe storage of data is critical for the safety and security of a user.

5.2.5 False Information

Should users be allowed to input false information?

Users may want to hide their real identities and those of their partners not only to eavesdroppers but also to other entities involved in the process. For example, a user may use an alias so that certain parties involved in the location service would see that somebody called Jon Doe is within a three mile radius of a store, whereas in reality Jim Rowe is the person that is actually in that perimeter. The user might also manipulate which component or derived measure of information is to be released to whom and in which granularity or accuracy in order to claim they were at some place at some time where they were not. There is probably little need or desire for developers to address potential misdirection activities by users.

5.3 Summary

In short the benefits of the model are that it provides customers the ability to decide their own ideal level of privacy, allows a customer to change her mind, addresses location privacy in a more comprehensive manner than policy based or minimum standard approaches, and provides customers with the assurance necessary to substantially increase demand for such services.

Among the potential drawbacks are that the implementation could be complex, industry is likely to be skeptical to provide such a system as it would reduce control and cut into current profits, and it could be years before the benefits from an implementation might be reaped.

CHAPTER 6

CONCLUSIONS AND FUTURE WORK

This chapter begins by summarizing the previously discussed work, then goes on to discuss complementary research topics that might be worthy of pursuit in the near future.

6.1 Thesis Summary

This thesis:

- introduced the issue of privacy in general and more specifically privacy issues in LBS environments,
- discussed various LBS technologies such as ETOD, GPS and others,
- outlined several scenarios where the above technologies could pose a problem to personal information privacy,
- explored several policy-based and minimum standard approaches such as IETF's "Geoprivacy requirements" and LIF's "Privacy Guidelines",
- described the core ideas of our model, which arose from the Platform for Privacy Preferences (P3P) concept,
- detailed a new dynamic contract-based approach that empowers the user to control his/her privacy, and
- analyzed the model from several different angles and addressed common issues and questions that have arisen in the research process.

The next section lends closure to this project by setting the stage for future work in this research area.

6.2 Thesis Conclusions

The previous chapters have outlined the conceptual model in a detailed manner and brought the evolution of the model to date. It is expected that the model will continue to evolve and be improved as more research is conducted. There are many potential directions to explore for protecting privacy in location-based services. Our major objective was to create an operational vision supporting user controlled protection of privacy that can help direct technological efforts along appropriate paths. We believe the research to be a good starting point for helping people to think outside the box and explore alternative ways for addressing privacy. At this point in time, there is no operational system for testing the validity of the model and discovering if it actually helps bolster the robustness of location-based service environments and make them more attractive to consumers. However, common sense and evidence from the literature suggests that user control over privacy has the potential for meeting the needs of significant number of LBS users. The next section discusses future research directions that have arisen from this project.

6.3 Future Work

The area of research addressed by this thesis is somewhat new compared to many traditional GIS and computer science research domains. Hence, future work in this line of research is rather limitless at this time. The next section explores just a few basic

conceptual frameworks that could develop in well-defined research initiatives given time and effort. Some of these topics such as uncertainty, ubiquitous computing and privacy in sensor environments are already being taken up by other researchers.

6.3.1 Uncertainty and Mobile Object Databases

Uncertainty involves the impreciseness or inaccuracy of information. In our case one of the examples of uncertainty is the location of the user's "personal communicator". Traditional databases contain static attributes that change upon an explicit update to the database. The value of a static variable is the same at any time as the value of the variable at time zero. Each query returns only what the user demands, not a whole range of answers. Therefore uncertainty does not play a major role in traditional DBMS. However, mobile object databases are a completely different case. The user does not usually know the exact answers, such as what is accurately solved and what is not solved. In mobile object databases the answers to our queries can return a single value or any set of values. And we do not usually know the exact solution. This is because, most times we are trying to model the future in MODs and querying the future is often uncertain by nature.

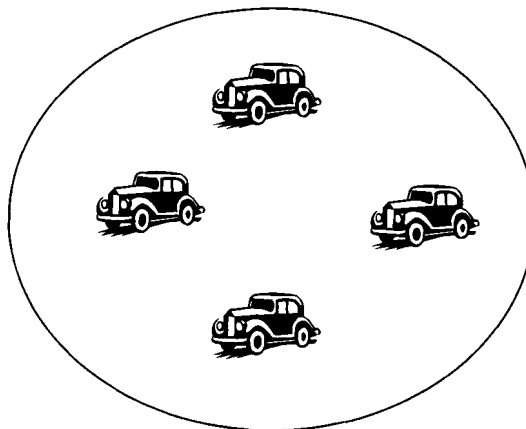


Figure 6.1 – Uncertainty in Location

What we understand from the above Figure 6.1 is that at any given time t our mobile object database could return an entire set of possible locations of a moving object (in this case the car). The query returns the circle and the object could be at any point within the circle, but we do not know exactly where it is. The size of our circle depends on the application domain being modeled in any particular scenario as well as the resolution of the available data. In an emergency response system we would prefer to have little location uncertainty. The sensitive nature of the application domain requires the information to be as accurate as possible. On the other hand we could tolerate a fair bit of uncertainty in an application such as a van distributing marketing brochures. Hence, it might be fruitful to address uncertainty in such a way that researchers consider the nature of the application being used. One might think that this is hardly an issue with GPS, but most LBS cell phone companies are still struggling to comply with certain aspects of E-911. ETOD is one of the most common network based location-fixing methods used, and thus uncertainty comes into play. Reducing uncertainty is already a key concern for many researchers (Sistla, Wolfson et al).

6.3.1.1 Strategies for Handling Uncertainty in MODs

Staying with the above line of thought, one strategy that has been researched for reducing uncertainty is **Bayesian Networks**. Bayesian Networks use probabilistic causal maps or belief networks. These networks are used when causality plays a role in a situation, but our understanding is limited or incomplete. In other words uncertainty exists. Hence we need to describe and model such situations through probabilities. In a typical Bayesian

network causality may exist between objects or they could also be independent of each other.

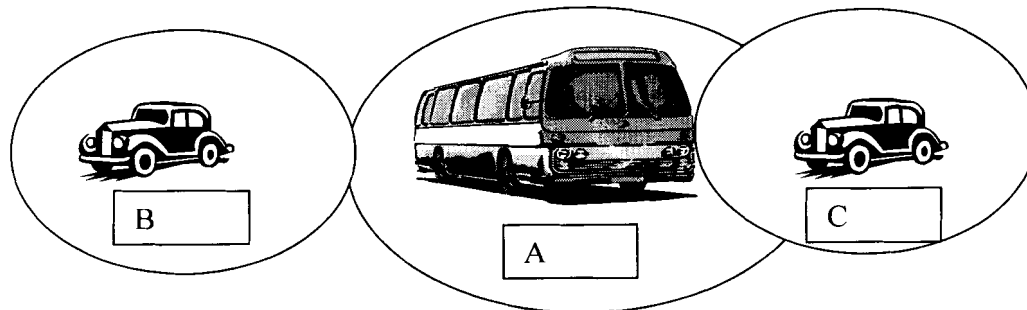


Figure 6.2 – A Bayesian Networks Example

Figure 6.2 illustrates Bayesian Networks in a rudimentary fashion in terms of location prediction and modeling. Let us consider the following query. Retrieve all taxis that will be within 100 meters of bus A in the next 5 minutes. The current location of the bus A is represented by the circle surrounding the bus. And the locations of the taxis are the circles surrounding the taxis. In five minutes (t_5), the location sets of the two taxis and the bus intersect, but as we notice taxi C has a much larger intersection than taxi B. Therefore the probability that taxi C will be within 100 yards of the bus location is fairly high, on the other hand the probability that taxi B will be within 100 yards of the bus location is fairly low. Now we can implement this probability set into some sort of threshold algorithm that would only accept certain probabilities and reject the rest due to the uncertainty surrounding those results. Therefore, if a Bayesian Network is implemented our query might only return taxi C even though our model suggests that taxi B could also be included in the query result. However, the uncertainty regarding taxi B is very high and hence we chose not to include it. This is one way of handling uncertainty in mobile object databases.

6.3.1.2 Other Considerations in Mobile Object Databases

In some instances an application prefer to keep a certain amount of uncertainty in a model to reduce the cost of operations. However, the tipping point between uncertainty and cost may be difficult to determine. For example the lower and upper bounds of speed might be germane in a specific application. Suppose the difference between the two is 10 MPH (miles per hour) in case 1 and 2 MPH in case 2. Case 1 would have to be updated much less frequently than case 2, because a car is more likely to overshoot the 2 MPH threshold than it would the 10 MPH threshold. Therefore case 1 is the cost effective model, but the uncertainty is fairly high. In case two, the uncertainty is much lower, but the cost of operations is increased dramatically. The idea is to find an optimal balance between uncertainty and cost. Advances in each of the uncertainty problem domains could be relevant to the practical implementation of the model suggested by this thesis.

6.3.2 Ubiquitous Computing

Ubiquitous computing is the concept of computers being omnipresent and embedded in our natural movements and interactions with our environment. “Ubiquitous computing is about interconnected hardware and software that are so ubiquitous that no one notices their presence.” (Weiser 2002) This concept is rapidly moving forward with conceptual and technological advances in mobile and pervasive computing. The advent of wireless telecommunications, high bandwidth networks and powerful microchips are bringing it closer and closer to reality. However this environment cannot achieve its

optimum operational potential until several **technological, organizational** and **social** issues are addressed.

The benefits of ubiquitous computing include that it has the potential to enhance knowledge work in an organizational setting, has increased ability to receive and process organizational data, and could help eliminate spatial and temporal boundaries such as office space and office hours. The shortcomings of ubiquitous computing include that personal group dynamics would be non-existent or difficult to support, unnecessary interruptions and biased decision making could result, a system that fits everybody would be difficult to achieve, the environment blurs context in archived digital communications, and there is the possibility of reducing separation between professional and personal life (Weiser 2002).

Privacy and the ownership data generated in ubiquitous systems are problematic. Ubiquitous computing has a very bright future only after these issues are addressed. Most technological issues are bound to be solved given time, but it is necessary to create a strong conceptual framework that accommodates social and organizational issues in order to fully utilize the technological advances.

6.3.3 Sensors and Privacy

Protecting privacy in the use of sensors has many parallels in protecting privacy in the use of LBS. Much sensor information will have a location component but not always. "Sensor network technology promises a vast increase in automatic data collection capabilities through efficient deployment of tiny sensing devices. Arrays of sensors could be deployed alongside roads to monitor traffic patterns or inside buildings to sense

contextual information for adaptive computing services.” (Gruteser et al 2003). Advances in sensor networking create significant privacy risks similar to those outlined in this thesis. Privacy is ever critical in these technologies, especially with the emergence of biosensors that can be embedded in or attached to human beings. Consistent with previous observations, privacy is typically addressed through privacy policies, which inform the user about a service provider's data handling practices and serve as the basis for the user’s decision to release data. This is another domain, where there is need for comprehensive privacy research. It is important to note that the characteristics of this domain may differ from location-based services and the privacy model would have to be customized to fit the complex nature of events. We believe that our LBS privacy model has broad ranging promise and could be applied to this domain, while considering the specific customizations that would be essential for sensor networks. (Gruteser et al 2003) propose a distributed anonymity algorithm that is applied in a sensor network before service providers gain access to the data (Gruteser et al 2003). In their opinion, these mechanisms can provide a high degree of privacy, save service users from dealing with service providers' privacy policies, and reduce the service providers' requirements for safeguarding private information. Researchers are currently pursuing several initiatives involving privacy in sensor networks and their work is likely to be critical to the applications that follow the development of these technologies.

6.4 Final Words

LBS environments are dynamic and therefore approaches need to be developed that are capable of responding to this dynamic nature. In protecting privacy our expanding

capabilities need to be able to accommodate both the technological and social components of society.

REFERENCES

- Agre, P.E. and Rotenberg, M. (1998). *Technology and Privacy: The New Landscape*. Cambridge, MA, The MIT Press.
- Alridge, E.C. (2001) *The Global Positioning System*. Los Angeles, CA, The Aerospace Corporation.
- Alsop, S. (1998). Where I'm Calling From. *Fortune Magazine*. Technology Buyer's Guide Special Issue: 34-35.
- Baum, D. (2001). The Ultimate Jam Session. *Wired Magazine*: 17-181.
- Bennahum, D. S. (2001). Here: Forget the World Wide Web on your Cell Phone. The Key to Wireless Internet Comes Down to Three Things: Location, Location, Location. *Wired Magazine*: 158-163.
- Benson, J. (2001). LBS Technology Delivers Information Where and When It's Needed. *Business Geographics* 9: 20-23.
- Bethell, A. (2002). *Evaluating Conflicts in the Development and Use of Geographic Information Systems*. Thesis, Dept. of Spatial Information Science and Engineering, Orono, University of Maine.
- Bhaduri, A. and Onsrud, H.J. (2002). User Controlled Privacy Protection in Location-Based Services. *Proceedings of the Second International Conference on Geographic Information Science (GIScience 2002)*. Boulder, Colorado, USA. University of California Regents.
- Birkin, M. Clarke, M. Clarke, G. and Wilson, A. (1996). *Intelligent GIS: Location Decisions and Strategic Planning*. London, GeoInformation International.

- Buchanan, M. (2002). *Nexus*. New York, London, WW Norton and Company.
- Center for Democracy & Technology. (2001). *Wireless Location*, Center for Democracy & Technology. 2001.
- Clarke, R. (1998). Platform for Privacy Preferences: A Critique. *Privacy Law & Policy Reporter* 5(3): 46-48.
- Clarke, R. (1998). Platform for Privacy Preferences: An Overview. *Privacy Law & Policy Reporter* 5(2): 35-39.
- Clarke, R. (1999). Person-Location and Person-Tracking: Technologies, Risks and Policy Implications. *Proceedings of the 21st International Conference on Privacy and Personal Data Protection*. Hong Kong: 131-150.
- Clarke, R. (2001). P3P Re-visited. *Privacy Law & Policy Reporter* 7(10).
- Cuellar, J. and Ersue, M. (2002). IETF: Geoprivacy Requirements, Internet Draft. Available: <http://www.ietf.org/ietf/1id-abstracts.txt>
- Curry, M. R. (1995). GIS and the Inevitability of Ethical Inconsistency. In *Ground Truth: The Social Implications of Geographic Information Systems*. New York, The Guilford Press.
- Davis, G. B. (2002). Anytime/Anyplace Computing and the Future of Knowledge Work. *Communications of the ACM* 45(12 (Special Issue on Ubiquitous Computing)): 67-73.
- Dempsy, J.X. and Mulligan, D. (2001). *Comments of the Center for Democracy and Technology*. Washington, DC.

Dennis, M. (2001). Location, Location, Location. Sun Microsystems 2001.

Dobson, J. (1993). Consider Both Sides of GIS Ethics. GIS World 6: 20-21.

Dobson, J. (1998). Is GIS a Privacy Threat? GeoWorld, July 1998.

Ericsson Website (2002). Available: <http://www.ericsson.com>

ESRI Support Website (2002). Available: <http://www.esri.com/support>

Federal Communications Commission (FCC) (2001). Fact Sheet: FCC Wireless 911 Requirements. Washington, DC.

Federal Trade Commission (FTC) (1999). Self-Regulation and Privacy Online: A Report to Congress.

Francica, J. R. (2002). LBS Technologies: Powerful Solutions Looking for a Market. GeoWorld, April 2002.

Fujii, K. (2001). iMode: The First Successful Smart Phone in the World. Japan, NTT DoCoMo.

Gattiker, U. et al. (1996). The Internet and privacy: Do you know who's watching? Business Quarterly 60(4): 79-84. Available: OVID: Accession Number: 01244444.

Geocanada Website (2001). Available: <http://www.geocan.nrcan.gc.ca/geomatics>

Gidari, A. (2000). No "L-Commerce" Without "L-Privacy": Fair Location Information Practices for Mobile Commerce. L-Commerce 2000 - The Location Services & GPS Technology Summit, Washington, D.C.

Gidari, A. and Altschul, M. (2000). Petition to the Federal Communications Commission by the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices. Washington, DC.

GIS Monitor. (2003). What Are Location-Based Services Anyway? GIS Monitor Newsletter, February 2003.

Goodchild, M. F. (1997). Uncertainty in Geospatial Information Representation, Analysis and Decision Support. NURI Research Proposal, submitted by NCGIA at the University of California, Santa Barbara and the University of Maine.

Grudin, J. (2002). Group Dynamics and Ubiquitous Computing. Communications of the ACM 45(12 (Special Issue on Ubiquitous Computing)): 74-78.

Gruteser, M. Jain, A. Han, R. and Grunwald, D. (2003). Privacy-Aware Location Sensor Networks. Boulder, CO, Department of Computer Science, University of Colorado at Boulder.

Guruduth, B. and Bernstien, A. (2002). Software Infrastructure and Design Challenges. Communications of the ACM 45(12 (Special Issue on Ubiquitous Computing)): 92-96.

Gutzman, A. D. (2001). Location-Based Services for Here, There, and In Between. Available: <http://www.mcommercetimes.com/Services/81>

Hoofnagle, C. J. (2002). Consumer Privacy in the E-Commerce Marketplace 2002. Internet Law & Business.

Huaiqing, W. Lee, M. K. O. and Wang, C. (1998). Consumer Privacy Concerns about Internet Marketing. Communications of the ACM 41(3): 63-70.

IBM Website (2002). Available: <http://www.ibm.com>

Jain, A. (2001). Implementing Advanced Location Enabled Applications. IBC Mobile Location Services, Rome, Italy.

Jessup, L.M. and Robey, D. (2002). The Relevance of Social Issues in Ubiquitous Computing Environments. Communications of the ACM 45(12 (Special Issue on Ubiquitous Computing)): 88-91.

Jurvis, J. (2001). Location's Where It's At. Rainer Technology, Inc. 2001.

Lee, J. H. (2001). Spatial Uncertainty Management Based on a Bayesian Network Model. Department of Information Science and Telecommunication, University of Pittsburgh.

Lessig, L. (1999). Code and Other Laws of Cyberspace. New York, Basic Books.

Lowe, J. W. (2001). The Power of Babble: Congregating around LBS, Geospatial Solutions. 2001. Available: <http://www.geospatial-online.com/0201/0201net.html>

Lyytinen, K. and Yoo, Y. (2002). Issues and Challenges in Ubiquitous Computing. Communications of the ACM 45(12 (Special Issue on Ubiquitous Computing)): 63-66.

Magellan Website (2002). Available: <http://www.magellan.com>

Monmonier, M. (2002). Spying with Maps: Surveillance Technologies and the Future of Privacy. Chicago, London, The University of Chicago Press.

Motorola Website (2002). Available: <http://www.motorola.com>

Mountain, D. and Raper, J. (2001). Positioning Techniques for Location-Based Services: Characteristics and Limitations of Proposed Solutions. Department of Information Science, City University, London.

National-Research-Council (2003). IT Roadmap to a Geospatial Future. Washington, DC, The National Academies Press.

Niedzwiadek, H. (2001). E-Business Embraces Location. *Business Geographics* 9: 18-21.

Nokia Website (2002). Available: <http://www.nokia.com>

Oinonen, K. et al. (2002). LIF Privacy Guidelines, Version 0.5.0.

Online Privacy Alliance. (2001). Guidelines for Online Privacy Policies. Available: <http://www.privacyalliance.org>

Onsrud, H.J (1993). GIS and Privacy. GIS/LIS' 93, Minneapolis, MN.

Onsrud, H. J., J. Johnson, and X. Lopez (1994). Protecting Personal Privacy in Using Geographic Information Systems. *Photogrammetric Engineering and Remote Sensing* 60(9): 1083-1095.

Onsrud, H.J. (1998). Tragedy of the Information Commons. *Journal of Policy Issues in Modern Cartography* (Elsevier Science): 141-158.

Onsrud, H.J. (2001). Research Proposal for SmartMaps Project. Available: <http://www.spatial.maine.edu/~onsrud/Research/privacy.pdf>

Onsrud, H.J. (2001). Contract Approach to Addressing Privacy in the Use of Location Based Services. Center for Spatially Integrated Social Science: LBS Specialist Meeting, Santa Barbara, CA.

Onsrud, H.J. (2003). Privacy in the Use of Spatial Technologies: Ethics as a Driver of Technological Research Priorities, NSF Confidentiality Workshop, May 12-13, 2003, Washington D.C. Available: <http://www.urban.org/nsfpresentations/index.html>

Onstar Website (2002). Available: http://www.onstar.com/us_english/jsp/index.jsp

P3P (2003). Platform for Privacy Preferences (P3P) Project, World Wide Web Consortium. Available: <http://www.w3.org/P3P/>

Privacy Working Group: Information Policy Committee. (1995). Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, Information Infrastructure Task Force.

Raper, J. (2002). The Dimensions of GIScience. Presentation at the Second International Conference on Geographic Information Science (GIScience 2002). Boulder, Colorado, USA.

Rothfeder, J. (1992). Privacy for Sale. New York, Simon and Schuster.

Schwartz, J. (2001). Privacy Issues Emerge from Wireless Location Technology. Navglobe: Journal of Global Navigation and Wireless Communication.

Seimens Website (2002). Available: <http://www.seimens.com>

Siewiorek, D. P. (2002). New Frontiers of Application Design. Communications of the ACM 45(12 (Special Issue on Ubiquitous Computing)): 79-82.

Sistla, A. Wolfson, O. Chamberlain, S. and Dao, S. (1997). Modeling and Querying Moving Objects. Proceedings of the 13th IEEE Conference on Data Engineering (ICDE), 1997. Birmingham, U.K.

Sonnen, D. (2001). What Does the Future Hold for Mobile Location Services? *Business Geographics* (9,1): 14-17.

Spinello, R. (2000). *Cyber Ethics: Morality and Law in Cyberspace*. London, Jones and Bartlett Publishers International.

Spinney, J. (2001). *LBS Technological Directions*. Center for Spatially Integrated Social Science: LBS Specialist Meeting, Santa Barbara, CA.

Sykes, C. (1999). *The End of Privacy: The Attack on Personal Rights at Home, at Work, On-Line, and in Court*. New York, St Martin's Griffin.

TechTarget (2001). *Location-Based Services*. Available:
http://searchnetworking.techtarget.com/sDefinition/0,sid7_gci532097,00.html

U.S. Senate Judiciary Committee. (2002). *Privacy in the Digital Age: A Resource for Internet Users*, Available: <http://judiciary.senate.gov/oldsite/privacy.htm>

VanderMeer, J. (2001). Will Wireless Location-Based Services Pay off? *Location Content Drives Wireless Telecommunications*. *Business Geographics* (9,2): 16-19.

Weitzner, D. J. (2000). *New Wireless Web Architectures: Function & Policy Implications*. Federal Trade Commission Workshop on Mobile Wireless Web, Data Services and Beyond, Washington, DC.

Whereonearth. (2001). *What are Location Based Services?* Available:
<http://www.whereonearth.com/lbs/>

Whitaker, R. (1999). *The End of Privacy: How Total Surveillance Is Becoming a Reality*. New York, The New Press.

Wright, T. (1995). Eyes on the Road: Intelligent Transportation Systems and Your Privacy, Information and Privacy Commissioner / Ontario.

APPENDIX A

PRIVACY LAWS

Compiled “as is” from the Location Interoperability Forum Privacy Guidelines (Oinonen et al 2002).

EU

In 1995 and 1997, the EU enacted two directives in order to harmonize data protection laws throughout the EU, to ensure citizens’ adequate levels of privacy protection and to allow free flow of personal information throughout the member states. In July 2000, an additional proposal was issued to provide further privacy protection in the electronic communications sector.

The Data Protection Directive from 1995 sets the benchmark for the processing of personal information in electronic and manual files and the movement of such data.

The Telecommunications Directive from 1997 sets the benchmark for privacy protection in telephone, digital television, mobile networks and other telecommunications systems. It provides additional privacy protection to EU citizens by imposing obligations on carriers and services providers. The directive sets restrictions on access to billing information and marketing activities, and it gives consumers the option to block their phone numbers. Additionally the directive requires carriers and service providers to delete information related to a call once the service is completed.

A new proposal, "The Directive on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector", issued in July 2000 will replace the Telecommunications directive and further strengthen privacy protection in the

EU once it is accepted. The proposed directive provides a broader perspective of electronic communications and it will ensure protection of all information transmitted across different electronic communications media, prohibit unsolicited e-mail without opt-in consent, and protect mobile phone users from location tracking and surveillance.

All EU member states are required to enact implementing legislation that follows the EU directives and provide independent bodies (a data protection commissioner or agency) to ensure the enforcement of the rules.

The directives impose an obligation on member states to ensure that personal information relating to EU citizens has the same level of protection when the information is exported and processed in countries outside the EU. This requirement has resulted in a growing pressure in many countries outside the EU, including the U.S., to enact stronger privacy protection laws.

US

There is no explicit right to privacy in the U.S. Constitution. A limited constitutional right to privacy is provided by the Fourth Amendment's protection against unreasonable search and seizure. The U.S. has no comprehensive privacy protection law for the private sector and no independent privacy oversight agency. Instead, self-regulation and sectoral laws have been adapted to protect consumers' privacy.

The best known of the federal laws is the Children's Online Privacy Protection Act, which went into effect in May 2000. The Act applies to commercial web sites that are directed to, or that knowingly collect information from, children under 13. With certain exceptions, these sites will have to obtain parental consent before collecting, using, or

disclosing personal information from children. Under the Act, sites must give parents a choice as to whether their child's information can be disclosed to third parties, and give parents a chance to prevent further use or future collection of personal information from their child. Parents must also, upon request, be given access to the personal information collected from their child and a means of reviewing that information.

The Communications Act of 1934 (47 U.S.C., Section 222) states that carriers have duty of confidentiality to the customer, and that they can use customer proprietary network information (CPNI) only in provisioning services requested by the user. CPNI information cannot be used for any other purpose without the written authorization from the customer.

The Wireless Communications and Public Safety Act of 1999 further amends Section 222 of the communications act to protect consumer location privacy and states that carriers must have "express prior authorization" from customers in order to use CPNI information (including location data) for marketing purposes.

The Financial Services Modernization Act allows users to opt-out from the usage and sharing of their data for marketing purposes. The bill however permits banks, insurance agencies and stockbrokers to merge their databases, providing these organizations access to more detailed customer information than previously. Law previously prohibited affiliation of these businesses.

Negotiations between the U.S. and the EU on the "Safe Harbor Principles" started in 1995 when the EU threatened to cut off all data flows, which is essentially most record of business transactions between the continents, unless the U.S. could guarantee that EU citizens' privacy would remain protected in the hands of American companies.

EU commissioners suggested the U.S. Congress should adopt privacy laws similar to the EU directives, while U.S. officials promoted self-regulation, or industry codes that U.S. companies would follow on pain of punishment of the FTC. An agreement was reached in April 1998 and took effect in November 2000. The agreement set out the following rules: U.S. companies can write contracts with privacy commissioners in the EU that lay out how they will protect personal data entrusted to them, or they can follow the Safe Harbor Principles, modelled after the EU Directive privacy protection rules. Enforcement of the Safe Harbor rules would be carried out by private groups and backed by the FTC.

Canada

In Canada the Personal Information Protection and Electronic Documents Act of 2001 gives certain rights with respect to the collection, use or disclosure of personal information by federally regulated organizations. These include airlines, banks, telephone companies, cable television and broadcasting companies. The Act applies to personal information collected, used or disclosed in the course of commercial activities, whether in the "real" world or on the Internet. It also applies to personal information disclosed to another province or country for profit or gain, where the information is the subject of the transaction.

Australia

The Privacy Amendment (Private Sector) Act 2000 regulates the way the private sector organizations can collect, use, keep secure and disclose personal information. It gives individuals the right to know what information an organization holds about them

and a right to correct that information if it is wrong. Consumers have the right to know *why* a private sector organization is collecting their personal information, *what* information it holds about them, how it will *use* the information and who else will *get* the information. Except for some special circumstances, consumers can ask to *see* this information and for the information to be *corrected* if it is wrong. Consumers can also make a *complaint* if they think their information is not being handled properly.

New Zealand

New Zealand is the only country outside of Europe with a comprehensive data privacy law, and it covers both government and business. New Zealand's law gives consumers access to their personal data, and it follows OECD guidelines. There are no data transport restrictions against countries with inadequate or no privacy policies. Instead New Zealand is trying to build an international environment toward compatible privacy policies among nations.

Japan

Japanese parliament appears poised to pass overarching legislation aimed at establishing a fundamental national privacy framework.

Latin America

Argentina is discussing about privacy with other members of the Mercosur South American trade pact, Brazil, Paraguay, and Uruguay, and with Internet groups in Chile, Bolivia, and Peru to develop a Latin American e-commerce framework.

APPENDIX B

CODE FOR MOCK UP SOFTWARE

```
' frmMain
```

```
Option Explicit
```

```
Private Sub cmdPhone_Click()
```

```
    Me.Hide
```

```
    frmPhone.Show
```

```
End Sub
```

```
Private Sub cmdPreferences_Click()
```

```
    Me.Hide
```

```
    frmPreferences.Show
```

```
End Sub
```

```
Private Sub cmdExit_Click()
```

```
    End
```

```
End Sub
```

```
Private Sub Form_Load()
```

```
    MsgBox "Please walk through the following set 'Personal Communicator' preference settings. Please use your mouse to make selections. This sequence of screens demonstrates how a 'Personal Communicator' user could be allowed to establish their own privacy preference settings and continually alter them 'on the fly' as desired or needed. An article describing the use of this demo can be found at
```

```
http://www.spatial.maine.edu/~anuket/research.htm ", , "Instructions, Please Read"
```

```
End Sub
```

```
' frmAnyone
```

```
Option Explicit
```

```
Private Sub cmdBack_Click()
```

```
    Me.Hide
```

```
    frmUser.Show
```

```
End Sub
```

```
Private Sub cmdExit_Click()
```

```
    End
```

```
End Sub
```

```
Private Sub cmdSelect_Click()
```

```
    Me.Hide
```

```
    frmMain.Show
```

End Sub

' frmBusinessList

```
Private Sub cmdBack_Click()  
Me.Hide  
frmUser.Show  
End Sub
```

```
Private Sub cmdExit_Click()  
End  
End Sub
```

```
Private Sub cmdSelect_Click(Index As Integer)  
Me.Hide  
frmMain.Show  
End Sub
```

' frmBusinessPref

```
Private Sub cmdBack_Click()  
Me.Hide  
frmUser.Show  
End Sub
```

```
Private Sub cmdExit_Click()  
End  
End Sub
```

```
Private Sub cmdSelect_Click(Index As Integer)  
Me.Hide  
frmMain.Show  
End Sub
```

' frmClient

```
Option Explicit  
Private Sub cmdExit_Click()  
End  
End Sub
```

```
Private Sub cmdBack_Click()  
Me.Hide  
frmPreferences.Show  
End Sub
```

```
Private Sub cmdSelect_Click()
```

```
Me.Hide  
frmMain.Show  
End Sub
```

```
Private Sub Form_Load()  
    cmdSelect.BackColor = vbYellow  
    cmdSelect.Caption = "Main Menu"  
End Sub
```

'frmConsumer

```
Private Sub cmdBack_Click()  
Me.Hide  
frmPreferences.Show  
End Sub
```

```
Private Sub cmdSelect_Click()  
Me.Hide  
frmMain.Show  
End Sub
```

'frmEmergency

```
Option Explicit  
Private Sub cmdBack_Click()  
    Me.Hide  
    frmPreferences.Show  
End Sub
```

```
Private Sub cmdExit_Click()  
    Unload frmMain  
    Unload frmEmergency  
    Unload frmAnyone  
    Unload frmUser  
    Unload frmServers  
    Unload frmClient  
    Unload frmPreferences  
    Unload frmOff  
    Unload frmDefinitions  
    Unload frmPhone  
End Sub
```

```
Private Sub cmdSelect_Click()  
Me.Hide  
frmMain.Show  
End Sub
```

```
Private Sub Form_Load()
```

```
'MsgBox "It is recommended that you specify phone numbers incase of emergency", ,  
""
```

```
End Sub
```

```
' frmOff
```

```
Option Explicit
```

```
Private Sub cmdSelect_Click()
```

```
Me.Hide
```

```
frmMain.Show
```

```
End Sub
```

```
Private Sub Form_Load()
```

```
'MsgBox "It is recommended that you choose the default settings", , ""
```

```
End Sub
```

```
Private Sub cmdExit_Click()
```

```
Unload frmMain
```

```
Unload frmEmergency
```

```
Unload frmAnyone
```

```
Unload frmUser
```

```
Unload frmServers
```

```
Unload frmClient
```

```
Unload frmPreferences
```

```
Unload frmOff
```

```
Unload frmDefinitions
```

```
Unload frmPhone
```

```
End Sub
```

```
Private Sub cmdBack_Click()
```

```
Me.Hide
```

```
frmPreferences.Show
```

```
End Sub
```

```
' Phone form
```

```
Option Explicit
```

```
Private Sub cmdClear_Click()
```

```
txtNumber.Text = vbNullString
```

```
End Sub
```

```
Private Sub cmdExit_Click()
```

```
Unload frmMain
```

```
Unload frmEmergency
```

```
Unload frmAnyone
```

```

Unload frmUser
Unload frmServers
Unload frmClient
Unload frmPreferences
Unload frmOff
Unload frmDefinitions
Unload frmPhone
End Sub

Private Sub cmdNumber_Click(Index As Integer)
    Select Case Index
        Case 0
            txtNumber.Text = txtNumber.Text & 0
        Case 1
            txtNumber.Text = txtNumber.Text & 1
        Case 2
            txtNumber.Text = txtNumber.Text & 2
        Case 3
            txtNumber.Text = txtNumber.Text & 3
        Case 4
            txtNumber.Text = txtNumber.Text & 4
        Case 5
            txtNumber.Text = txtNumber.Text & 5
        Case 6
            txtNumber.Text = txtNumber.Text & 6
        Case 7
            txtNumber.Text = txtNumber.Text & 7
        Case 8
            txtNumber.Text = txtNumber.Text & 8
        Case 9
            txtNumber.Text = txtNumber.Text & 9
        Case 10
            txtNumber.Text = txtNumber.Text & "*"
        Case 11
            txtNumber.Text = txtNumber.Text & "#"
    End Select
End Sub

Private Sub cmdPhonePref_Click()
    Me.Hide
    frmUser.Show
End Sub

Private Sub cmdSelect_Click()
    Me.Hide
    frmMain.Show

```

```

End Sub

Private Sub Form_Load()
    'Label1.GotFocus
    'cmdBack.Picture = 'back.ico'

End Sub

Private Sub cmdBack_Click()
    Me.Hide
    frmMain.Show
End Sub

' frmPreferences
Option Explicit
Private Sub cmdAnyone_Click()
    Me.Hide
    frmAnyone.Show
End Sub

Private Sub cmdBack_Click()
    Me.Hide
    frmMain.Show
End Sub

Private Sub cmdClient_Click()
    Me.Hide
    frmClient.Show
End Sub

Private Sub cmdDefinitions_Click()
    Me.Hide
    frmDefinitions.Show
End Sub

Private Sub cmdEmergency_Click()
    Me.Hide
    frmEmergency.Show
End Sub

Private Sub cmdOff_Click()
    Me.Hide
    frmOff.Show
End Sub

```

```
Private Sub cmdSelect_Click()  
Me.Hide  
frmMain.Show  
End Sub
```

```
Private Sub cmdServer_Click()  
Me.Hide  
frmServers.Show  
End Sub
```

```
Private Sub cmdUser_Click()  
Me.Hide  
frmUser.Show  
End Sub
```

```
Private Sub cmdExit_Click()  
Unload frmMain  
Unload frmEmergency  
Unload frmAnyone  
Unload frmUser  
Unload frmServers  
Unload frmClient  
Unload frmPreferences  
Unload frmOff  
Unload frmDefinitions  
Unload frmPhone  
End Sub
```

```
Private Sub Command1_Click()  
Me.Hide  
frmConsumer.Show  
End Sub
```

```
'frmServer2  
Private Sub cmdBack_Click()  
Me.Hide  
frmServers.Show  
End Sub
```

```
Private Sub cmdSelect_Click()  
Me.Hide  
frmMain.Show  
  
End Sub
```

```
Private Sub Command1_Click()
```



```
Me.Hide
frmServers.Show
End Sub
```

```
' frmServer
```

```
Option Explicit
Private Sub cmdExit_Click()
    Unload frmMain
    Unload frmEmergency
    Unload frmAnyone
    Unload frmUser
    Unload frmServers
    Unload frmClient
    Unload frmPreferences
    Unload frmOff
    Unload frmDefinitions
    Unload frmPhone
End Sub
```

```
Private Sub cmdSelect_Click()
Me.Hide
frmMain.Show
End Sub
```

```
Private Sub Command1_Click()
Me.Hide
frmServer2.Show
End Sub
```

```
Private Sub Form_Load()
    MsgBox "It is recommended that you choose the default settings", , ""
End Sub
```

```
Private Sub cmdBack_Click()
    Me.Hide
    frmPreferences.Show
End Sub
```

```
' frmUser
```

```
Option Explicit
Private Sub cmdBack_Click()
Me.Hide
frmPreferences.Show
End Sub
```

```
Private Sub cmdExit_Click()
```

End
End Sub

Private Sub cmdSelect_Click()
Me.Hide
frmMain.Show
End Sub

Private Sub Command1_Click()
Me.Hide
frmBusinessList.Show
End Sub

Private Sub Command10_Click()
Me.Hide
frmAnyone.Show
End Sub

Private Sub Command2_Click()
Me.Hide
frmBusinessPref.Show
End Sub

' **Splash Screen**

Option Explicit

Private Sub Form_KeyPress(KeyAscii As Integer)
 frmMain.Show
 Unload Me
End Sub

Private Sub Frame1_Click()
 frmMain.Show
 Unload Me
End Sub

Private Sub Timer1_Timer()
 frmMain.Show
 Unload Me
End Sub

BIOGRAPHY OF THE AUTHOR

Anuket Bhaduri was born in Bombay, India on November 17, 1978. He attended St. Lawrence High School and MMK Junior College for Commerce and Economics in Bombay. In September 1996, he headed for the University of Maine in Orono, U.S.A to pursue a Bachelor's degree in Management Information Systems and Financial Economics. After graduating in May 2001, he spent the summer working for Bankers Life and Casualty Co. in Bangor, ME. He joined the department of Spatial Information Science and Engineering in September 2001 as a graduate student and research assistant. Anuket is a candidate for the Master of Science degree in Spatial Information Science and Engineering from The University of Maine in August, 2003.