Master's Theses   Master's Theses and Graduate Research

2007

User-centric privacy control in location-based services

Kent Russell Bloomer
San Jose State University

Follow this and additional works at: https://scholarworks.sjsu.edu/etd_theses

USER-CENTRIC PRIVACY CONTROL IN LOCATION-BASED SERVICES

A Thesis

Presented to

The Faculty of the Department of Geography

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

By

Kent Russell Bloomer

May 2007

UMI Number: 1445222

INFORMATION TO USERS

The quality of this reproduction is dependent upon the quality of the copy
submitted. Broken or indistinct print, colored or poor quality illustrations and
photographs, print bleed-through, substandard margins, and improper
alignment can adversely affect reproduction.
 In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if unauthorized
copyright material had to be removed, a note will indicate the deletion.

UMI®
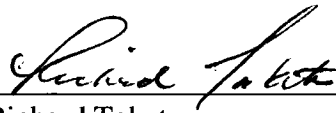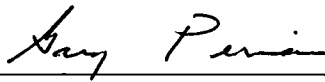
APPROVED FOR THE DEPARTMENT OF GEOGRAPHY

_____

Dr. Richard Taketa

_____
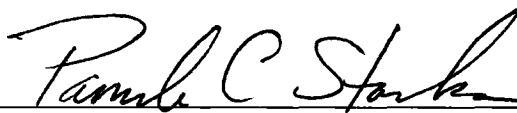
Dr. Gary Pereira

_____

Dr. Kathryn Davis

APPROVED FOR THE UNIVERSITY

_____

ABSTRACT

USER-CENTRIC PRIVACY CONTROL IN LOCATION-BASED SERVICES

Kent Russell Bloomer

The unprecedented level of popularity in mobile devices for communication purposes is driving a technological and social change. Mobile device technology is rapidly being developed and is currently being applied for location-determining purposes. Location-based services (LBS) allow users to deliver and receive information that is related to a particular location through wireless telecommunication. However, serious concerns are mounting about how privacy will be impacted by the inclusion of LBS technology in mobile applications. This thesis addresses the topic of the technology and also the privacy issues that are associated with LBS by proposing a conceptual model designed to control privacy from a user-centric environment.

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

viii

LIST OF FIGURES

CHAPTER 1

Introduction

Wireless and Global Positioning System (GPS) technology is rapidly being developed

and is currently being applied for location-determining purposes. The ability for

emergency departments to respond quickly to a scene is an excellent application of GPS

technology. However, GPS technology is being used for much more than to guide

emergency personnel. Telematics, the integration of wireless communications, vehicle

monitoring systems, and location devices, provides a wide variety of additional services

(mobiledia 2004). GPS and cellular technologies are being combined to create

geographic information system (GIS) services for private businesses such as

vehicle/container monitoring, truck/tractor fleet management, on-board security tracking

and remote diagnostics. These technologies have been proven to be useful.

1.1 Problem Area

Within the broader field of tracking technologies, location-based services (LBS) are a

subset of capabilities that allows users to deliver and receive information that is related to

a particular location through wireless telecommunication (Markkula 2001). Serious

concerns are mounting about how privacy will be impacted by the inclusion of intelligent

spatial technology in mobile applications. For example, cellular carriers, under a federal

mandate, are required to pinpoint the location of a wireless 911 call within 100 feet

(FCC, 1996). The problem is with balancing the need of emergency workers to be able to

pinpoint the locations of 911 callers, while at the same time, honoring the need of private

1

callers to protect their privacy and location. The potential for misuse and abuse of personal location information generated by such technologies is what concerns some people. For example, marketing agencies gathering information by monitoring a user's personal habits could be interpreted by that user as an invasion of privacy. Users of LBS are increasingly concerned over the privacy and accuracy of confidential information, the unsolicited information that comes their way, and the ownership and control of location information. To reduce these privacy concerns and risks, protection capabilities need to be accounted for from the outset in the design and coding of intelligent spatial technologies (Onsrud et al 2004).

1.2 Problem Definition

Consumer concerns about privacy erosion is the most serious obstacle to the potential growth of LBS (Markkula 2001). This thesis evaluates the attributes of both wireless location-based technologies and services, and the protection of an individual's right to privacy. This thesis discusses the road map of legislation protecting privacy rights, whether the objectives were met or not, and addresses the potential challenges with future legislation. This thesis also reviews the attempts made by others to construct a regulatory framework to protect privacy in LBS. The problems and concerns connected with security and the question of data ownership will be explored.

The primary objective of this thesis is to develop mechanisms for interacting with data to provide for a user-controlled environment that will increase support for the individual. The hypothesis of this thesis is that the development of a user-centric approach in the use of LBS better supports privacy protection than current approaches. In an effort toward

reaching this goal, a conceptual model will be developed and analyzed. The model objectives are:

- Research components of LBS and the technological feasibility of implementing the proposed model.

- Develop a comprehensive privacy preference framework that supports primary LBS contexts and addresses ownership of personal information.

- Develop input controls to express privacy preferences. For example, at what distance do I want to be located and under which circumstances?

- Implement the system on resource constrained (size, weight, memory, etc.) devices.

- Secure the exchange of personal information through access controls (e.g., user name/password). The aspects of this objective will be developed from a user-side perspective. An overview of some provider-side aspects of identity management will be outlined.

Ideally, a dynamic interaction would develop between service provider and user. This will be challenging given the way in which standards have been developed, where the service provider already has considerable control over developing privacy standards. However, by addressing this issue proactively, a constructive solution with a balanced control system in which privacy concerns are addressed at a user level may encourage LBS growth.

In the case of LBS, the issue is not so much whether these services should proceed, but rather how, where, and to what extent. Although the law has recognized a reasonable expectation of privacy in a public place, albeit a limited one, the courts have recognized that individual privacy is a basic prerequisite for a democratic society. An individual's sense of freedom rests on governmental respect for privacy. Therefore, all efforts for implementing location-based technologies and services must recognize and respect the individual's expectation of privacy.

1.3 Related Work

This thesis analyzes the technical feasibility of developing user-controlled mechanisms to manage privacy for LBS. With the anticipated growth of LBS a plethora of research has been focused on developing a variety of solutions for enforcing privacy. This brief overview of related work is by no means intended to be extensive. The intent here is to point out some of the areas of research that are most closely related to the topic of this thesis.

With the proliferation of mobile devices capable of accurately reporting their position in space and time, research and development of spatio-temporal masks are promising. Pfoser and Jensen (1999) propose a framework for incorporating privacy protection into LBS consisting of two types of spatio-temporal masks based on the inherent uncertainties in tracking data: measurement and sampling. Measurement masks function on observed locations. These masks intentionally distort the location through an error inducing function that moves the true position to a new location. Sampling masks introduce

uncertainty in modeling continuous moving objects. Controlling the number and timing

of observations allows for hiding the location of an object between samples.

Markkula (2001) proposes a new service infrastructure, called Dynamic Geographic

Data Service (DGDS), designed for collecting, managing and releasing dynamic

geographic data. Typically users are required to grant access to the location of their

mobile equipment (ME) to each LBS provider. All of the LBS providers then have the

ability to identify the user, and can collect some identifiable information about the user.

Figure 1.1 illustrates a general LBS data flow with the addition of the intermediate

positioned DGDS. The DGDS operates as a mediator in the sense that its primary task is

to collect personal data from heterogeneous sources and transform them into

unidentifiable data. When the data are not identifiable, regulations concerning privacy do

not apply and the data can be released to external third parties.
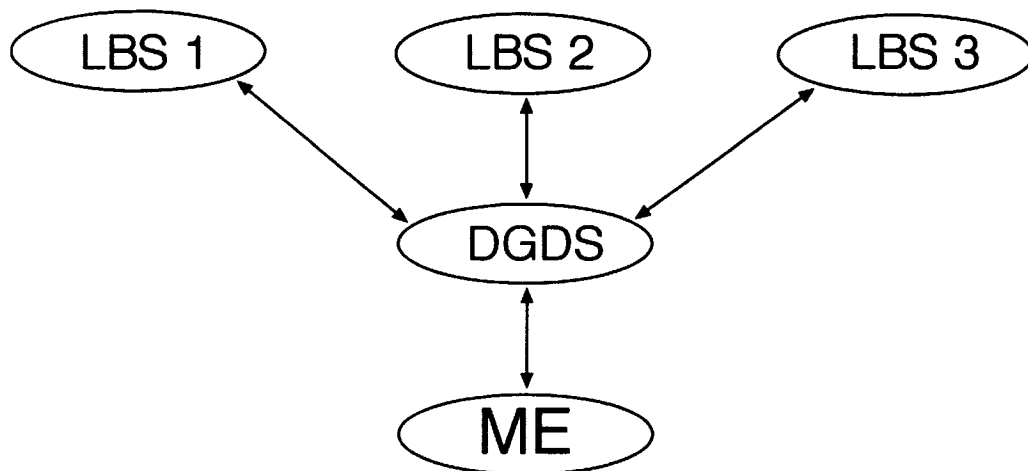
Figure 1.1: DGDS architecture

CHAPTER 2

Privacy

Despite the multitude of academic papers and legislation devoted to the subject of privacy, the concept of privacy remains difficult to define. Definitions include: "the right to be left alone," "the right to exercise control over information about oneself," and "the ability to control the use and disclosure of one's personal information" (Daon 2003). Conflicts arise between opposing interests because of the many different definitions and interpretations. Many of the commonly perceived views regarding privacy are at odds with the technological society in which we live, where personal information, such as credit card and license numbers, age, weight, height, etc., is disseminated through wired and wireless transmission and audio processing. As a result, today's world presents issues of privacy that were not previously considered in documents such as the US Constitution and Bill of Rights. Given the ramifications of not providing a strong protection of privacy rights, it is not surprising that the public as a whole has a vested interest in identifying what constitutes privacy.

2.1 Information Flow and Privacy Risk

Many samples of mobile GIS programs from major vendors are available that offer different functions and features and serve different applications. A good example, for purposes of explaining a practical LBS application, is automobile navigation. The recently emerged automobile navigation and emergency response system equipment that some luxury cars provide, is a set of innovative services to car owners. These on-board

systems help drivers navigate unfamiliar roads, identify the location of lost or stolen cars, and provide safety and convenience services.

The physical components that permit such field devices to operate are independently manufactured but installed by the automobile manufacturer or as an after market product by a suitably qualified and experienced person. When a new automobile is purchased, owners have the option to subscribe, for a fee, to a service provider. The automobile company or owner then subcontracts with this service provider. The service provider, in conjunction with the cellular carrier, actuates the field device. A national cellular carrier provides the cellular airtime for the field device and sends bills to the service provider. The service provider then forwards these bills to clients.

OnStar, a General Motors-owned service provider, is the largest supporter of LBS for vehicle drivers with more than 2 million subscribers (OnStar 2004). The OnStar telematics system combines vehicle control and monitoring systems with location tracking and wireless telecommunications. Each device is controlled through a three-button console: (1) a red emergency button, which sends a priority signal to an advisor who can send help to your location, (2) a white button for personal calling, and (3) a blue button for all other safety and convenience services. An additional feature, stolen recovery mode, allows an OnStar representative to open a cellular connection to a vehicle and listen to oral communications within the car (The Company 2004). This feature provides assistance in locating and retrieving stolen cars, as well as aiding law enforcement agencies fighting criminal activity.

In one such case, law enforcement ordered OnStar to intercept conversation. The Ninth Circuit U.S. Court held that the service provider and cellular carrier could be ordered to assist the Federal Bureau of Investigation (FBI) in intercepting these oral communications under 18 USC.§ 2518(4) of the Omnibus Crime Control and Safe Streets Act of 1968. Title III of the Act requires telecommunication carriers to "furnish [law enforcement] ...all information, facilities, and technical assistance necessary to accomplish [an] interception" (CCPIS 2003). By understanding the origin of such laws, we can review the regulation of electronic surveillance and see how legislation protects privacy rights.

2.2 Data Ownership

The privacy challenges over ownership, accessibility, and distribution of data are complex and multi-faceted. Many privacy advocates argue that location tracking devices are owned by the purchaser and thus own the data as well. If this holds true, then the ability to access data will be greatly reduced under certain circumstances. For instance, when an employer provides an employee with a mobile device, only the employer has the ability to access the data. Additional problems arise when data is shared at intermediate stages of data transmission such as cellular and service providers.

According to current legislation, data from these providers may be lawfully intercepted by law enforcement agencies. For example, Lojack, an automobile security system service provider, tracks and recovers stolen vehicles, but the technology extends to provide law enforcement agencies with a multitude of features and benefits that may or may not include tracking a stolen vehicle. If Lojack should try to limit the amount of

8

information they are willing to share, law enforcement agencies have the authority to then require the cellular provider to furnish additional information. Furthermore, although LBS companies are scrutinizing third-party data processors, like never before, consumers continue to be wary of data sharing and security breaches.

2.3 Privacy Strategies

The focus in this section is on mechanisms and processes that regulate the management of personal information. Three general approaches for regulating privacy in LBS applications are: through law, technology, and self-regulation, or some combination of these approaches.

2.3.1 Legal Regulation of Electronic Surveillance: An Overview

In order to understand the most recent laws, in particular the significance of the USA Patriot Act (USAPA), some familiarity with the history of electronic surveillance laws is necessary to have. This section will summarize the evolution of electronic surveillance laws through an assessment of case law and the statutory environment.

2.3.1.1 Federal Communications Act

The Federal Communications Act of 1934 contained the first federal regulation of wiretapping, stating that:

> .....no person not being authorized by the sender shall intercept
> any communication and divulge or publish the existence, contents,
> substance, purport, effect, or meaning of such intercepted
> communications to any person (Cotler and Larson 2001).

However, this law didn't specifically forbid law enforcement agencies or the government from wiretapping.

2.3.1.2 Katz v. United States

In the 1967 Supreme Court case, *Katz v. United States*, 389 US347 the court

recognized that eavesdropping on a conversation made from a public telephone was a

violation of privacy. Prior to *Katz*, the Supreme Court had regarded wiretapping as

outside the scope of the Fourth Amendment's restrictions on unreasonable searches and

seizures.

2.3.1.3 Omnibus Crime Control and Safe Streets Act

One year later Congress enacted the Omnibus Crime Control and Safe Streets Act

(Omnibus Act) of 1968. Title III of the Act, Wiretapping and Electronic Surveillance,

made the first attempt at regulating communications privacy and electronic surveillance.

Title III surveillance is a traditional wiretap that allows law enforcement agencies to bug

rooms, listen to telephone conversations, or get content of electronic communications in

real time (EFF 2001). This Act clarifies the procedures and techniques by which law

enforcement officials could obtain and conduct electronic surveillance.

2.3.1.4 Electronic Communications Privacy Act

The 1986 Electronic Communications Privacy Act (ECPA) was passed in response to

the growing number of technologies enabling electronic data transfer. In addition,

privacy advocates were calling for clear protection from law enforcement agencies

gaining access to a growing number of databases. Up to this point, legislation was aimed

at increasing privacy protection while providing law enforcement's ability to intercept

communications.

2.3.1.5 Communications Assistance for Law Enforcement Act

In 1994, however, the Communications Assistance for Law Enforcement Act

(CALEA) was signed into law, marking a change in legislation, to promote law

enforcement agencies ability to conduct electronic surveillance. As a result of CALEA

legislation, telecommunications companies are required to ensure that their technologies

do not impede law enforcement interception of communication (Cotler and Larson 2001).

This legislation mandates, in effect, that telecommunications carriers must take steps to

ensure that the technological advancements in the industry do not eliminate law

enforcement access to communications of targeted individuals.

2.3.1.6 Wireless Communications and Public Safety Act

The Wireless Communications and Public Safety Act of 1999 enhanced public safety

by encouraging and facilitating the deployment of a nationwide communications

infrastructure for emergency services. In effect, the Act directed the Federal

Communications Commission (FCC) to implement the Enhanced 911 (E911) program to

serve as a universal emergency assistance number for mobile phone users. Emergency

response agencies could be routed to a particular scene through position-determining

equipment (PDE). Difficulties in deploying such a system have been slower than

planned. Although handsets manufactured after February 3, 2000 must be equipped with

GPS technology, some cellular carriers are not yet capable of accurately locating callers

as required (FCC 2001). Privacy advocates argue that E911 represents a threat to privacy

because location-tracking technology is forced on mobile phone users.

2.3.1.7 Location Privacy Protection Act

In the wake of the September 11th terrorist attacks, the proposed Location Privacy

Protection Act of 2001 died in committee. The Act would have extended FCC regulation

to all providers of mobile services, including LBS. Unlike current law the proposed Act

would have required wireless carriers to notify their clients before releasing any

information to third parties. The Act died, in large part, because the committee was

concerned that the growth of developing technologies for LBS would be constrained

(White 2003). Furthermore, the committee may have been concerned that by

strengthening privacy rights, they would inadvertently constrain law enforcement

agencies' ability to fight the war on terrorism.

2.3.1.8 USA Patriot Act

On October 26, 2001, President Bush signed the USAPA into law. As a result of this,

domestic law enforcement and international intelligence agencies' powers have been

significantly increased. This law is a tremendous blow to ordinary American's civil

liberties, especially the right to privacy in our wired and wireless communications and

activities. Previously the government could spy on those already under criminal

investigation, now however, the person spied on does not have to be the target of the

investigation (EFF 2001). Furthermore, Internet service providers (ISPs) are encouraged

and sometimes required to hand over online communication information about users to

the government. The bill is a large and complex law intended to make America a safer

society, yet we have little evidence to substantiate that claim. Civil liberties have been

compromised because of bad intentions from a small number of individuals. However,

the benefits and consequences from this bill have not yet been fully recognized. The

USAPA expired on December 31, 2005 and can only be renewed by Congress. The

concern now is the review by Congress and the subsequent provisions that are made and

to what extent.

2.3.1.9 Can-Spam Act

With the passing of the Can-Spam Act in 2005, sending any electronic message to the

end user without the end user specifically opting-in became illegal. This put an

additional challenge on LBS applications as far as network-centric services were

concerned. As a result, a focal point on developing user-centric LBS and applications has

emerged, which give the user control of the experience (Olesen 2005).

2.3.2 Technical Solution

Privacy-enhancing technology (PET) solutions for LBS are technical representations

of a perception of the meaning of privacy (Camp and Osorio 2003). PET can be divided

into five categories:

- *Anonymizers* are tools that strip out personal information in order to protect user

  privacy.

- *Proxies and firewalls* are barriers between a device and the server that allow

  communications only under certain circumstances and block certain types of

  communication entirely.

- *Cookies* are small text files saved on the drive by a web site when visited and then

  are retrieved when the web site is revisited. These files identify an individual's

13

device and record the preferences and other data about the visit to that site so that

when the site is revisited, the visit is personalized.

- *Pixel tags/Web bugs* are small, graphic images on a web page or in an email

  message that are designed to monitor who is reading the web page or email

  message.

- *Encryption tools* enable the user to scramble data to protect the contents of emails

  and online communications. This type of software enables an individual to

  protect stored files and authentication issues.

These PET tools have proven to be useful, but they tend to give users a false sense of

privacy (Ang 2001; Froomkin 2000). Clients also have to assume that service providers

abide by their policy standards.

2.3.3 Self-Regulation

The United States has relied more on self-regulation than legislation. The problem

with self-regulation is that there are no clear solutions of enforcement, limited in scope,

vary widely, and that regulation becomes more difficult with larger and more diverse

LBS. Also, by developing a plethora of regulation standards through numerous groups

the situation becomes more complicated and therefore detracts from resolving the privacy

issues. Developing a set of uniform and consistent privacy standards that can be widely

accepted and applied by both industry and users is a promising solution, but has proven to

be difficult. And then there is the question of who will regulate the regulators?

2.4 Recent Policy-based Strategies

If we can agree that privacy protection on an individual basis is extremely important,

then a legal, technical, and regulatory framework that facilitates the use of LBS, while preserving individual rights, can resolve the bulk of privacy issues. An active and informed decision process at the individual and business levels could further assist in this cooperative effort. This could be manageable, in part, if businesses recognize the importance of privacy and take necessary steps to protect data belonging to their customers. Several businesses have joined to form working groups to address these issues. The following section will review attempts made by the Wireless Location Industry Association, Platform for Privacy Preferences Project, and GeoPriv workgroup to protect privacy in LBS.

2.4.1 Wireless Location Industry Association

The Wireless Location Industry Association (WLIA) has established guidelines for member companies to adhere to, setting acceptable standards for protection of the individual privacy of subscribers to LBS that can be located by using signal location technology (WLIA 2001). The WLIA is particularly interested in promoting industry self-regulation. The standards contain conduct guidelines for members and include:

- The LBS provider will use the data for intended purposes.

- Require explicit consent from the client.

- Notify clients of the privacy policy guidelines when entering a business relationship.

- Ensure personal and location data is accurate and secure.

- Allow clients to access and update any stored personal information.

- Refrain from storing personally identifiable information for longer than is necessary

to supply services.

- Not engage or condone wireless spam.

The following problems exist with this sort of privacy and position policy. The LBS has an agreement with the network operator, but not with the client. In other words, clients cannot determine which services can target them. An alternative approach would require the creation of some kind of blacklist. This can make things even more complex since some sort of encryption may need to be implemented. As a client a user would be continuously prompted to respond to requests. As a result of this inconvenience, subscription to such services may decline.

In many cases the client may not be the user. For example, employees of corporate businesses are frequently supplied with cellular phones. The idea of a system of constant surveillance may worry employees. If a user has the ability to make a direct agreement with the service provider, however, a client can decide whether or not to be positioned.

2.4.2 Platform for Privacy Preferences Project

The Platform for Privacy Preferences Project (P3P) is an initiative, proposed by the World Wide Web Consortium (W3C), intended to allow users to create policies for how the information they gave out should be used. This system enables users to retrieve a standardized set of multiple-choice questions, covering all the major aspects of a website's privacy policies, which then determines how the information will be used. Once the P3P enabled browser has read the preferences, the user can then decide to decline or accept the transfer of personal information on those terms. At a minimum, the P3P system enhances user control by providing access to their preferences. Although no

16

solid solutions ensuring privacy for mobile systems exist, important points have been emphasized in several W3C workshops (P3P 2005).

The first, and most important of these points is that the user must be in control of personal information. Granting access of control, however, is a crucial—and difficult— issue. Secondly, privacy tools and privacy architectures must be further developed. Although few tools exist a variety of possible tools need to be built into the system. In addition, architectures must be designed in a way that allows users to control access to their personalization profile. An analysis reveals some negative aspects of the P3P initiative. They are:

- Privacy terms for a particular transaction provide no means to ensure enforcement of the stated privacy policies.

- How to handle third party data collection on websites is not addressed.

- Privacy protection for users is limited by setting relatively low privacy preference defaults.

- User has to accept an "as is" policy or disconnect from the server.

2.4.3 GeoPriv Protocol

GeoPriv is a workgroup of the IETF (Internet Engineering Task Force) addressing the questions of authorization, integrity, security, and privacy in location-aware applications. The group has created a policy-based system, much like P3P, by setting up a framework and architecture so that clients and servers can pass around geographic location information by attaching privacy rules to that information. The work group relies on currently available devices and technological capabilities rather than development of new

technologies and techniques to protect individual privacy. Although the project utilizes

an already established protocol and format standard, a key task will be to enhance this

format to ensure that the security and privacy methods are available to LBS applications

(IETF 2005).

An additional approach being developed by the IETF includes transmitting location-

related objects in an extended Presence Information Data Format (PIDF), which was

designed for communicating privacy-sensitive presence information (Peterson 2004).

The PIDF object extensions carry secured information in how the data can or cannot be

used and by which entity it was designed for. The entity may have control over the

policy, however the target (mobile device) may not be owned by the entity. For example,

a company may own and provide a mobile device to an employee but the company can

set the privacy rules.

The workgroup has developed a draft focusing on user-controlled policies

(Schulzrinee et al 2004). The model includes a set of rules that describe the permissions

given by users of LBS. The user is able to specify which attributes of information are to

be applied and at what level of accuracy. The policy rules also specify conditions that

permit a LBS provider to process location information.

The GeoPriv drafts are a step in the right direction but more steps are necessary in

order to produce a comprehensive solution. However, several other drafts under

consideration will be available for review in the future. The shortcomings are similar to

the P3P concepts and include the inability for the user to interact and change policy

preferences without an explicit update request. Furthermore, since the LBS companies

are involved in the proposed policy solutions, several issues are left open to broad interpretations that may favor their interests.

2.5 Security

Security and privacy may be confused because they are not the same things, but they are inextricably related. Secure information is not accessible for unauthorized parties, while private information is not accessible without permission. Therefore, the service provider must effectively and actively integrate privacy and security management strategies to ensure privacy.

Using anonymity to preserve privacy is especially important when applications from third-party technologies such as *push/pull* services are employed. This requires security so that the anonymous information remains so during data transmission.

Security of information is best preserved if the following controls are implemented:

- *Authentication*: the verification of a claimed identity.

- *Authorization*: the process of validating the credentials of a person, computer process, or device.

- *Confidentiality*: the guarantee that data is not shared with unauthorized entities.

- *Integrity*: the guarantee that data has not been altered or destroyed in an unauthorized manner.

- *Nonrepudiation*: a technique used to ensure that someone performing an action on a device cannot falsely deny that they performed that action.

2.6 Summary of Privacy Approaches

An assessment of the approaches (legal, technical, and self-regulation) indicates that they are all valid. Although each approach has distinctive characteristics, this thesis primarily focuses on privacy and the use of LBS technology. However, this approach will not be sufficient in itself. A combination of all approaches will have to develop in some symbiotic form and will be discussed where appropriate.

CHAPTER 3

Location-Based Services Technology

A LBS in a mobile cellular network is a service provided to the subscriber based on their geographical location. The position can be determined through a radiolocation function, built into the cellular network or mobile device, that uses triangulation between the known geographic coordinates of the base stations through which the communication takes place (Agre 2001). Figure 3.1 illustrates a comprehensive overview of various technology and usability aspects of LBS.

3.1 Location-based Services Architecture

The applications of LBS are rapidly becoming developed. Understanding how these systems work and how they are used will help to assess and enhance data privacy and security. The general architecture of LBS includes three major components: the client, server, and network services (Figure 3.2). The client utilizes the services provided by the cellular service and mobile GIS content providers. The server provides the means to offer information-processing services and to rapidly distribute location information contents. The cellular service providers enable the wireless network linkage, facility, and equipment to provide air interfaces, networking, routing, and other communication services for mobile device users (Peng and Tsou 2003).

3.2 Position-determining and Processing Components

An overview of how a mobile client's location is derived requires an understanding of position-determining equipment (PDE) and position-processing technology. PDE

21

TECHNOLOGY

Position determination

High Accuracy | Low Accuracy

Indoors | Outdoors

Bluetooth WLAN | CGI-TA TOA AOA EOTD | GPS A-GPS

Database Management

Wireless link | Application level

SMS WAP GPRS | EMS MMS | Java SIM Tk Html

Terminal

Screen | Interface

B/W Color | Size 101x80 320x240 | GPS | Wireless

LOCATION BASED SERVICES

General Information Navigation instructions

Keypad Touchscreen | Privacy control Visualization tools Service acceptance | General information Abs. coordinates Routing instructions | Maps Routing Real time navigation | Friend finder Navigaton Location | Advertising

Personalization | Voice | Emergency

Menus | User controlled actions | Text | Graphical | User activated services | Push services

User Interface | Data Presentation | Services

USABILITY

Figure 3.1: Technology and usability aspects of LBS

identifies the location of the mobile device. Position-processing technology is a software

technology to process, track, and manage the location information sent from the PDE

(Peng and Tsou 2003). The implementation adoptions of the positioning methods depend

on the development of network operators, handset manufactures, and service providers.

The following sections discuss triangulation and trilateration, and various location-fixing

methods used to track mobile clients from one location to another. Information-

processing functions, such as graphic display, rendering, geocoding, proximity searching,

and routing are also discussed.

Satellites	Field Device	Cellular Tower	Cellular Carrier	Network	Server	Service Provider	Client/ Target

Internet
or
Direct Link

Vending Machine Reporting HVAC Equipment Control Security Systems Monitoring Vehicle / Container Tracking Oil, Gas, Electric Utility MonitoringVehicle Navigation	Signaling and messaging technology enables a communication link; AMPS CDMA, TDMA and GSM.	Determines the position of the mobile devices and makes data and applications available to the mobile client devices	PC Pocket PC PDA's Cellular Telephones

NAVSTAR is a constellation of 24 satellites, launched by the American Department of Defense. They are the satellites used by most GPS receivers to calculate your position.

The communication infrastructure that allows clients and servers to connect with one another.

Figure 3.2: General system architecture of mobile GIS

3.2.1 Triangulation

The triangulation method is sometimes used for cellular communications to determine

the geographic location of a mobile device. Triangulation is the process by which the

location of a radio transmitter is established by directions and/or calculating the

geometric and trigonometric relationship from two or more signal positions (TechTarget

2001). In general, a network-based system relies on triangulation of cellular information

in CDPD (cellular digital packet data) or a GPS-based system placed in the mobile device

23

(Peng and Tsou 2003). Figure 3.3 illustrates the process of triangulation. When time interval signals are detected and measured from the mobile device to two or more base stations, distance is determined. The lower portion of the illustration shows how base stations equipped with directional antennas can be used to locate a mobile device.

3.2.2 Trilateration

Unlike triangulation, trilateration uses the known locations of two or more reference points, and the measured distance between the subject and each reference point (Boertien and Middelkoop 2002). A variant of trilateration is hyperbolic positioning and will be discussed in the *time difference of arrival* (3.2.4.3) section.

3.2.3 Position-determining Satellite Solutions

Satellite solutions rely on the positioning software installed within a mobile device. The most commonly used satellite-based solutions include:

- Global Positioning System (GPS)

- Assisted Global Positioning System (A-GPS)

- Enhanced Observed Time Difference (E-OTD)

3.2.3.1 Global Positioning System (GPS)

GPS data input and analysis is one of the most exciting and important tools available today as the interest in LBS increases (ABI 2004). GPS data include the horizontal and vertical position based on the geographic grid or a coordinate system. Linear and polygonal features can be determined by a series of GPS positions.

Using satellites orbiting in space as reference points, a GPS receiver can determine a precise 3-D position on the earth's surface. The U.S. military maintains a network of 24

24
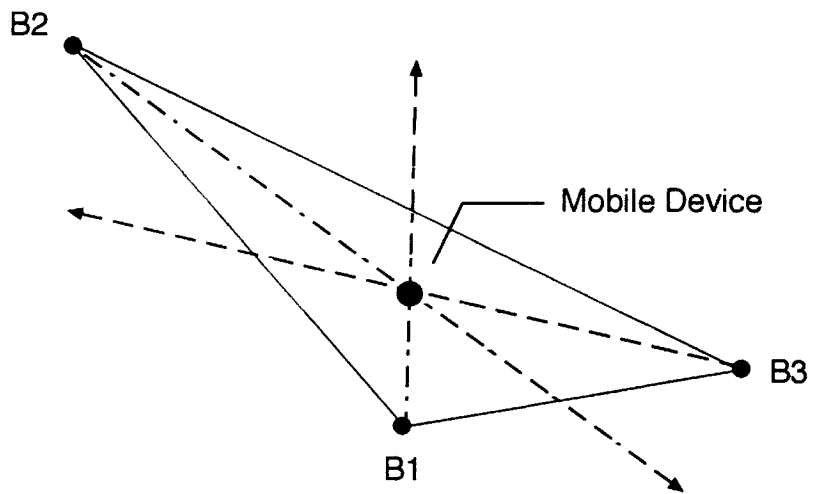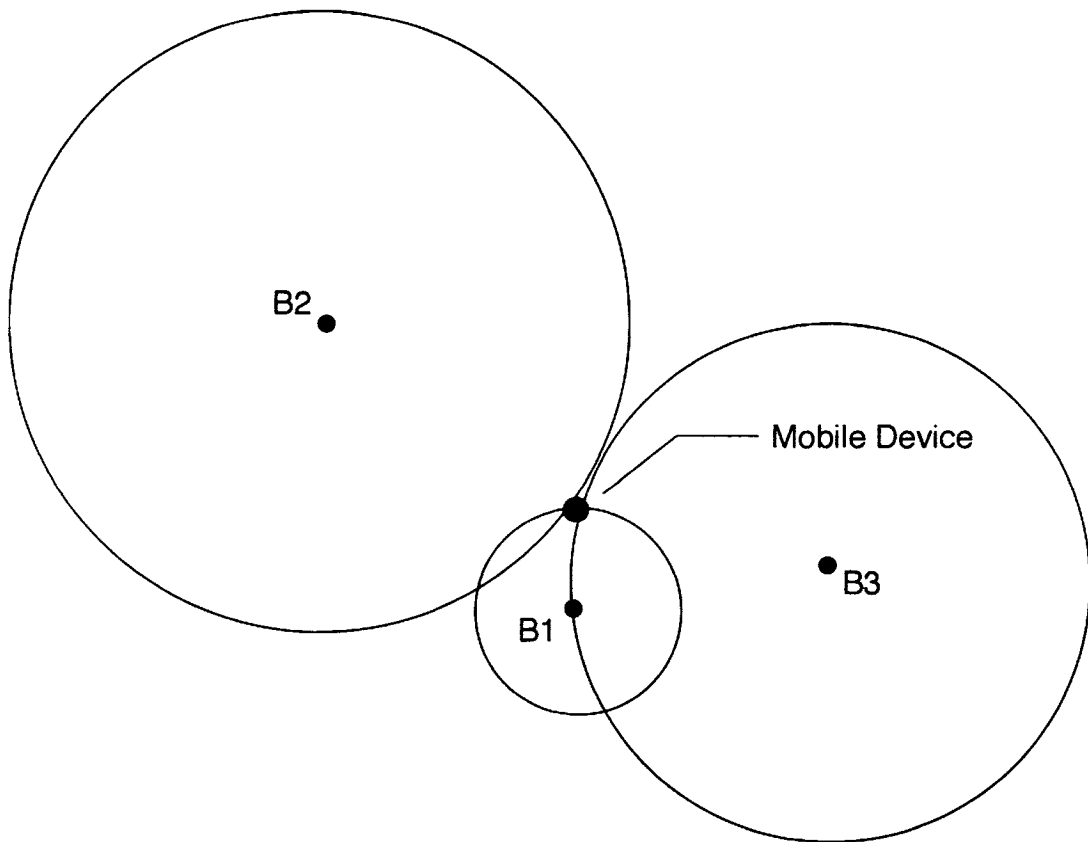
Figure 3.3: The process of triangulation

NAVSTAR (Navigation Satellite Timing and Ranging) satellites orbiting in space around the earth, forming an artificial constellation. Each satellite follows a precise orbit. The constellation provides GPS users between 5 and 8 visible satellites from any point on the earth's surface. The GPS finds the location by detecting signals from satellites at precisely timed intervals. Most GPS receivers are code-based and receive instantaneous positioning accuracy of around 5m-50m, depending on signal strength. Models equipped with differential correction can easily achieve 3-5m accuracy (Chang 2002).

3.2.3.2 Assisted Global Positioning System (A-GPS)

The A-GPS uses a network of fixed GPS receivers that are spaced within about 500 kilometers of a reference base station. The network of receivers provides information to the reference base station, through a cellular infrastructure, enabling a significant reduction in transmission time. The network components boost time-to-first-fix (TTFF) performance from a minimum of 18 seconds in a stand-alone system to a few seconds in an assisted system (LaMance, Desalas, and Jarvinen 2002).

3.2.3.3 Enhanced Observed Time Difference (E-OTD)

Another mobile terminal solution is the *enhanced observed time difference* (E-OTD), which relies on time-based signal measurements from multiple base stations to the software in the mobile device. The differences in time between these terrestrial-based reference points and the mobile device determine the user's location positioning and accuracy. The spatial and temporal data from three or more base stations is synchronized. Typically, data is synchronized through base stations equipped with stationary GPS receivers. Although signal availability is not affected by GPS, which is

reliant on a clear sky, the reception of radio frequency signal availability from the base station to the mobile device is impeded by the topography of terrain features. The horizontal positioning accuracy of E-OTD is expected to be around 125 meters (Andersson 2005).

3.2.4 Position-determining Network Solutions

Network solutions rely on PDE installed at switch centers. The most commonly used network-based solutions include:

- Cell Global Identity and Timing Advance (CGI-TA)

- Time of Arrival (TOA)

- Time Difference of Arrival (TDOA)

- Angle of Arrival (AOA)

Each solution uses the principles of triangulation, based on angular measurements, and trilateration, based on distance measurements, or some combination of both.

3.2.4.1 Cell Global Identity and Timing Advance (CGI-TA)

The *cell global identity* (CGI) solution determines the location of the cell coverage area of the user as the approximate location of the mobile device. The *timing advance* (TA) procedure assists with positioning and returns cell identification. Positioning is determined through a temporal measurement between the start of a radio frame and a data burst. Each base station within a cell is at a varying distance, and the bursts may arrive before or after their respected time slot, therefore bursts from each terminal must be adjusted accordingly through TA. The accuracy is limited to the cell size, which may vary from 10 to 500 meters (Anderrson 2005).

3.2.4.2 Time of Arrival (TOA)

The *time of arrival* (TOA) solution determines the mobile device location based on the intersection of three or more arcs (Figure 3.4). Time between the base stations and the mobile device (equivalent to distance) is measured in absolute time and calculated through synchronized clocks that compensate for timing errors. Each base station must have monitoring equipment installed, thus potentially being expensive to implement.
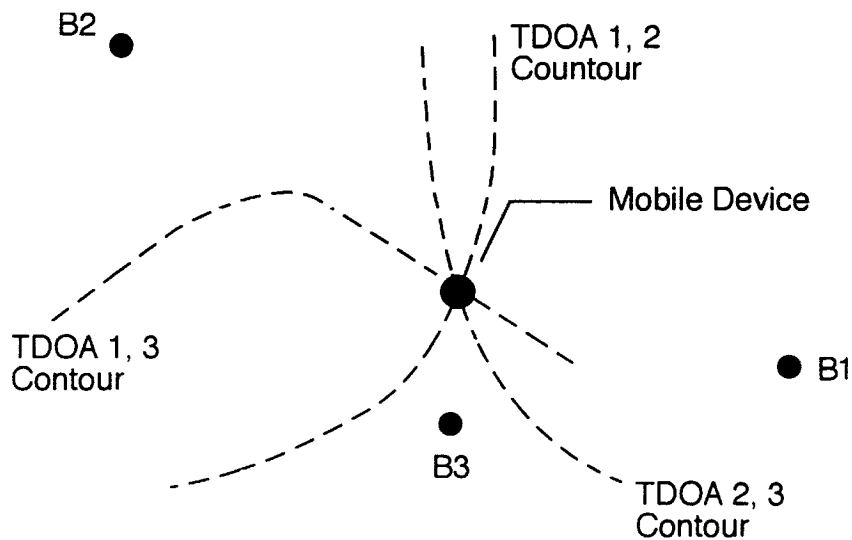
Figure 3.4: The TDOA geolocation process

3.2.4.3 Time Difference of Arrival (TDOA)

The *time difference of arrival* solution determines the mobile device location based on trilateration. Arrival time differences to each base station, rather than absolute time, is measured (equivalent to distance differences). To calculate time differences a hyperbolic

curve must be defined. The intersection at which the hyperbolas meet determines the

position (Figure 3.4).

3.2.4.4 Angle of Arrival (AOA)

The *angle of arrival* solution is based on the angle of signal arrival with respect to the

axis of an antenna array by at least two base stations. Each base station must have

directional antennas or an antenna array installed, and thus is potentially expensive.

3.2.5 Position-processing Technology

Position-processing technologies facilitate the network or server-side to process, track,

manage and help other applications to query and retrieve the geographic information sent

from PDE. Some of the common component functions in LBS are described in the

following sub sections.

3.2.5.1 Graphic Display

The basic function that a presentation component should provide is to display

geospatial data. Geospatial image display can either be in raster images or vector

(feature) data. Raster data is based on rows and columns of cells where each cell is

stored as a single value. Vector data is based on points (e.g., stores, restaurants, gas

stations); lines (series of point coordinates, e.g., streets, rivers, boundaries); and polygons

(shapes bounded by lines, e.g., parks, water body, vegetated land). Vector data can also

be used to represent continuously varying phenomena such as triangulated irregular

networks (TIN) and contour lines (Chang 2002).

3.2.5.2 Rendering

The *rendering* component should allow the user to adjust the zoom and pan values,

and to change the point of view. This will help users to view small screens.

3.2.5.3 Geocoding

Geocoding is the process that associates geographic references, such as parcels,

addresses, phone numbers, and postal codes, with location coordinates (e.g.,

longitude/latitude). The result of the geocoding is an interpolated, or estimated,

positioned point or feature. The points or features can then be mapped and entered into a

searchable database. *Enhanced geocoding* interprets or adapts user input for improved

results. *Reverse geocoding* is the process of returning an estimated geographic reference

point or feature as it relates to a given coordinate.

3.2.5.4 Proximity Searching

Geospatial *proximity searching* is the method of finding specific points of interest

(POI) associated with locations within a given distance of a specified destination (Peng

and Tsou 2003). For example, "alert me if I drive within one mile of a Starbucks coffee

house in the next hour."

3.2.5.5 Routing

Geospatial data combined with routing algorithms are calculated to determine optimal

routing information between two geocoded points. Once the results are generated several

options are presented to the user who then has the ability to initiate action, based on their

criteria (e.g., distance, time, scenic directions), and to complete the task. *Dynamic*

30

rerouting is the method of recalculating alternative travel routes and times, based on real-time traffic and other live feeds, to help travelers avoid congestion (Tele Atlas 2003).

3.3 LBS Technology Summary

Exploring the foundation of mobile positioning technologies, which is the key for enabling LBS applications, was essential for understanding LBS and how location data is transferred. The satellite solutions are the most widespread for obtaining location outdoors. Network solutions are more suitable for indoor environments. No matter what system prevails, we still need solutions for users to control privacy. The next chapter focuses on developing such a solution.

CHAPTER 4

User-Centric Conceptual Model for Privacy Protection

Different ways and strategies in how a model is designed and implemented affect the usability of a system. This chapter will define and demonstrate the design concepts and functionalities of the proposed solution.

The challenge with LBS is not in the applications but in the design and implementation. Every effort to increase the usability of the UCM (User-centric Model) will be made. The ability for the user to establish and update personal data would assure that information to each user is truly customized. However, human misuse or error in the comprehension, operation, and maintenance of information must be considered. Furthermore, the users need to understand their status and position relative to their preferences.

4.1 Conceptual Device

The more evolved conceptual device in this thesis can be referred to as a smartphone. A smartphone is defined as any electronic hand-held device that integrates the functionality of a mobile phone, personal digital assistant (PDA) or other information appliance (Yuan 2006). A palm-size or hand-held device is a good rule of thumb when envisioning an appropriate size limitation. Anything in excess of this probably qualifies as a laptop and is inappropriate for everyday LBS applications.

4.2 Self-provisioning Privacy Preferences

An important objective of the UCM is to provide user-control of personal information to determine ownership. The ability for a user to control their own personal information allows for user-defined ownership privileges. The server and their affiliates have the ability to entice users to use their services under terms that best serve them (if permitted). Authorization is granted at the discretion of a user to define rules that meet their needs. For example, if a user blocks advertising solicitations from a *push* service, the location-based server must enforce that rule.

This section outlines a general framework of the UCM, with an emphasis on privacy preferences for what, when, where, and how personal data should be shared. As illustrated in Figure 4.1 the user will have access through logically controlled access points: (1) LBS Server, (2) Clients of LBS Server, (3) Communication List, and (4) Public Safety. Each access point provides a series of settings further described in the following sections.
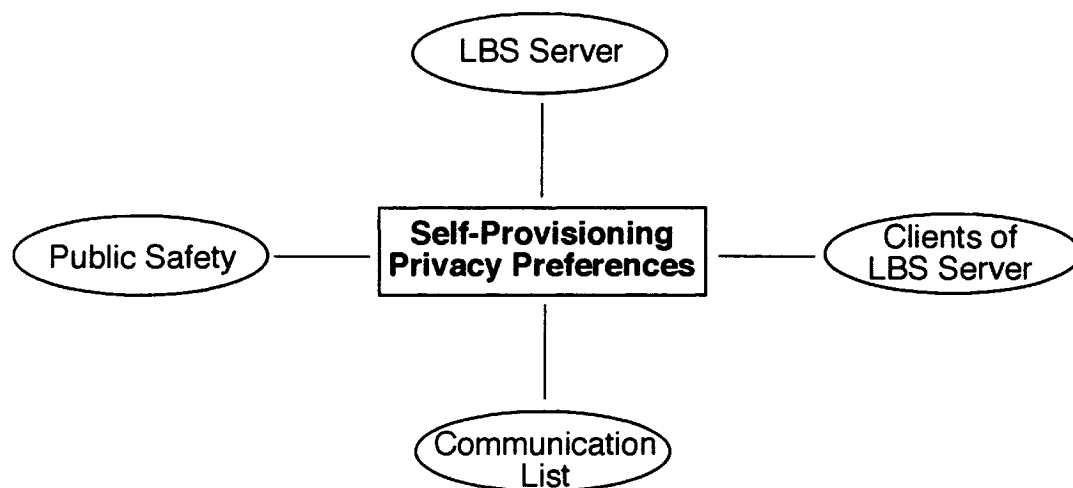
Figure 4.1: Logically controlled access points

33

4.2.1 LBS Server

To support dynamic personalization to the fullest extent, the user interface, where a

proper logic and data flow is managed, must be conceptually intuitive and designed for

speed and ease of use. The interface must also feature simple query entry, quick

navigation, and precise use of limited smartphone screen size. The menu in Figure 4.2

allows a user to express predefined or user-defined preferences from a list of varying

levels of privacy protection. A choice can be activated or deactivated by selecting a

LBS Server Access to Client

■ Deactivate   Ability to locate the client is not permitted

■ Low   Active: -- any distance
          Retain Location Records: -- continuous
          Transfer to Third Parties: -- always allowed

◎ Medium   Active: ·· within 50 feet ▼
          All preferences must be defined by the client,
          otherwise predefined default settings will be active.

■ High   Active: -- any distance
          Retain Location Records: -- never allowed
          Transfer to Third Parties: -- within entity boundaries

Figure 4.2: Multi-level preferences for LBS server access

color-coded button and, if applicable, specifying how information should be filtered. For

instance, in this example, a color-coded button in the menu displays green when

"medium" is activated and changes to red if deactivated. In addition to the medium level

of protection being activated, a user may further define settings through complete control

over descriptive numerical measures. For example, the user can change a distance parameter from 50 feet to 10 miles (Figure 4.3). Notice that greater distances introduce levels of location uncertainty as when a user expands from a precise location to a spatial unit. The three other settings do not allow a user to fine-tune attributes (i.e., settings are predefined). The "retain location records" data allows the server to retain records for a specified period of time, if any, for future services. In the context of the low level option, future services may include services from third parties since the "always allowed" option is stated. When the high level option is selected third parties can only contact a target if the target is within their business boundary.

The LBS server access menu is accompanied with a help icon denoted by a yellow "H". When activated, a search bar opens and the user types in a key word. For example, typing, "transfer to third parties," returns a list of attributes (e.g., notified, not notified) whereby the user clicks on a specific attribute and receives a detailed description. This type of menu layout addresses, in part, the issue of a limited screen size for display by breaking up relatively lengthy descriptions onto separate display windows.
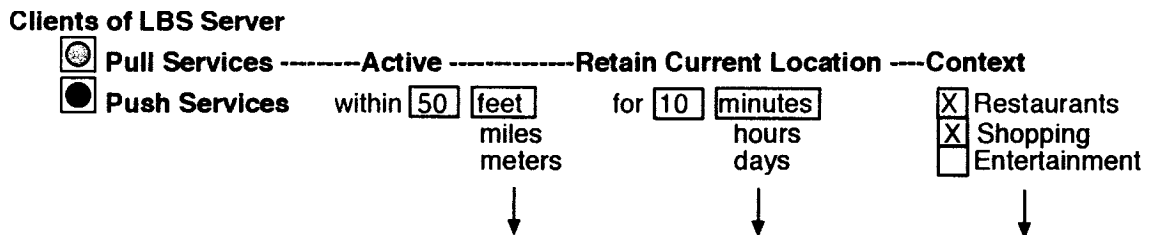
Figure 4.3: Self-provisioning preferences for LBS server clients

35

4.2.2 Clients of LBS Server

The menu in Figure 4.3 allows a user to select the services offered by the clients of the LBS provider. The clients want to know what the server knows. These clients are typically referred to as *push* and *pull,* or third party, marketers. *Push* and *pull* services are services that rely on the network's ability to locate subscribers. In a *push* service, wireless data are delivered to a user's mobile device without the user's request. An example of this is a person walking by a movie theater that receives a movie theater advertisement. In a *pull* service approach, wireless data are delivered to a user's mobile device upon their request; otherwise the server can't track the user. A typical example of this is when a user requests information on a specific movie. Depending on the requests, results can vary from movie times, locations, directions, tickets, coupons, etc. *Pull* services appear to be less intrusive to the user than *push* services. Furthermore, a recent study indicates that more than 68% of the participants polled are in favor of *pull* services rather than *push* services (Hassim and Gao 2002).

Communication List ----- Add Row
- ⊛ **Groups**
- ⊛ **Friends** -------Name ------ Add Row
- ● **Work**   Alex ----- **Address** -----------------Active
- ● **Family**   Ashley   211 Saxon Road   from 8:00 to 17:00 on Weekday
          Don   **Phone**   Weekend
      ↓   ↓   Home 831-462-9447   within 10   feet   Monday
             Mobile 831-345-2897   miles   Tuesday
             Work 831-476-3817   meters   ↓
             Email   kilometers
             Alx@hotmail.com

Figure 4.4: Self-provisioning preferences for communication lists

36

4.2.3 Communication List

The ability to establish and manage communication links between the user and contact

lists is illustrated in Figure 4.4. Selecting "add row" can create lists and their contents.

Once a "name" (Alex) has been created, in this example, additional information (e.g.,

address, phone numbers) is inserted via a device keypad. Notice that data such as

numerical measures may be separated from previous data and displayed onto a series of

pages for easier browsing on small-screen devices. The conceptual smartphone equipped

with a scroll wheel illustrates how the user would navigate through the pages (Figure

4.5).
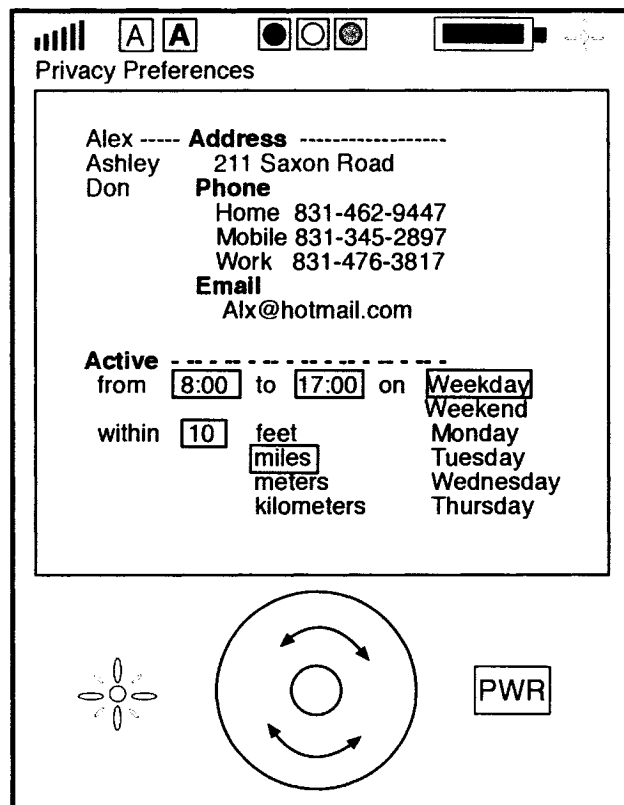
Figure 4.5: Conceptual device

4.2.4 Public Safety

The E911 requirement for tracking devices has a primary purpose of providing

immediate emergency assistance to individuals. A clear statement of this requirement,

optional emergency responders, and public safety related topics are illustrated in Figure

4.6. In addition to the mandatory E911 link between user and responder, the user may

Public Safety

☐ **E911** --------------- **Always Active**

◎ **Traffic Alerts**   This unit is equipped with Enhanced 911 (E911) technology which
●   allows for communication and your location to be determined by
● **Amber Alerts**   emergency responders.
● **Disaster Alerts**
    ↓   Additional E911 responders ------ [Add Row]
                               Charles ------ Phone
                               Monte   Home   831-462-9447
                               Tasha   Mobile 831-345-2897
                                              Work   831-476-3817

Figure 4.6: Self-provisioning preferences for public safety

establish a list of additional emergency responders that will have access to an open line of

communication. This system has the capacity to support multiple lines of communication

that may facilitate rescue efforts (Figure 4.7). For example, a person on the emergency

list may be able to provide pertinent information to the police. The integration of public

safety solutions such as traffic, Amber, and disaster alerts may also prove useful.

4.3 Usage and Default Scenarios

Usage pattern and default profiles play a crucial role in the personalization of LBS

(Wagner 2005). Under certain scenarios the user's request may not be fulfilled because

of a parameter limitation. To accommodate the full expressiveness of the user, the

38

Public Safety
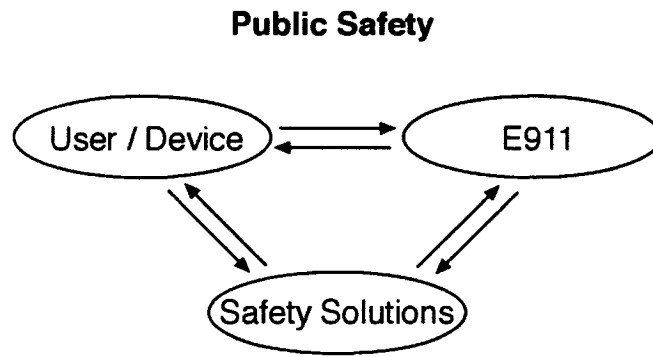
Figure 4.7: Flow of safety information

server will present the user with several options. For example, a user may typically be

willing to travel twenty miles to a movie theater. The "*pull* server," however, is unable to

provide any results for a specific movie because of a distance parameter defined in the

user's settings. To resolve this issue the server asks the user for permission to override

the existing setting. The prompt would read as follows:

Would you like to expand your search area?

- Permit once (predefined setting is retained).

- Always permit (this setting is changed to the default mode; there are no

   distance parameters).

- Never permit (you will not receive another prompt to modify settings for

   movie information).

Once the privacy preferences are modified the result is a refined profile that facilitates a

faster, safer, and more effective service. Notice that this system is partly defined by

rules, i.e., the server provides privacy options that are translated into rules.

4.4 Contract Language

Protecting the privacy of customers who use telecommunication networks is not a new endeavor. By law, all service providers use language in their contracts to maintain strict customer information privacy policies. However, the language relates to relatively static systems, rather than dynamic systems. In this UCM, an interactive conceptual language would be implemented to manage LBS privacy preferences. An excerpt from such a contract may read as follows:

> We, and our affiliates, will not share personal information about you with others without your permission. We have a duty under federal law to protect the confidentiality of information about the quantity, technical configuration, type, destination, and the amount of your use of our service, in relation to your interactive privacy preference settings. We can, however, share and use this information as required by law, by legal process, or by exigent (E911) circumstances. The altering of your privacy preferences will immediately take affect and be enforced by the server. Any interruption in service will automatically reset your privacy preferences to pre-programmed default settings. You are responsible for all levels of privacy as defined by you.

4.5 Model Summary

This proposed shift toward this new paradigm for managing LBS services is an extraordinary step, signifying a change that may have a profound impact on the way LBS services are governed and managed. Now that an increased clarity of the UCM is recognized several key benefits can be realized. The UCM provides an increased ability

for the user to control various levels of protection, allows for a plethora of user-defined

inputs with specified conditions for each, and provides an ability for the user to change

preferences on the fly to accommodate changing needs. By empowering the LBS user,

through the personal control over privacy, an increase for such services are likely and

therefore could encourage a shift in industry standards. However, implementation could

still be complex, given the way in which standards had previously been developed, where

the service provider already had considerable control over developing privacy standards.

The usability of the UCM is presented in the following chapter by providing an

operational usage scenario.

CHAPTER 5

Operational Usage Scenarios

The following chapter explores client usage scenarios, considering three levels of privacy, which users will express when using context-aware LBS.

5.1 Client Usage Scenarios

The Johnson family, consisting of Fred, Elinor, and their teenage daughter Alisha, has planed a trip to a comprehensive shopping mall. The mall offers LBS, which allows customers to access product information (location, price, and comparisons) in a time-efficient and cost effective means. The mall encompasses a large area equipped with an array of sensors and WiFi technology for service access.

The car's telematics system synchronizes with Fred's mobile device and automatically adjusts mirrors, seating, and climate controls, to his personal preferences. His mobile device also detects the navigation system and provides him with the mall address, driving directions, and approximate arrival time. While driving to the mall, Fred receives a traffic alert and is redirected to an alternate route. As they enter the crowded mall parking lot, Fred is directed, through the mall's LBS system, to a convenient parking space. The family exits the car and heads off into different directions.

- Fred enters the mall and is offered the LBS. He has never used the service and needs to define his privacy preferences. He is provided with general options such as: the user is willing to share personal information (bonus points/rewards, low protection); the user accepts that the LBS can request information defined by

42

user-specified accuracy and frequency parameters (free, medium protection); or

user-specific conditions (fee, high protection). He agrees to use the high

protection service but does not want to be bombarded by ads from all of the

businesses within the mall, only the ones he enters. He agrees to use the service

for a small one-time fee. A dialog box opens indicating the amount of the fee.

The next time he enters the mall his default setting will remain valid.

- Alisha's parents purchased a mobile device and service plan for her. She is

  interested in the services and doesn't see the harm in giving out her location

  information. All businesses within the mall will have the ability to locate her.

  They can also collect information that can be used for marketing purposes.

  However, her identity will be anonymous. As a reward she receives bonus points

  that can be used to purchase products at several of the stores she frequents.

- Elinor is a frequent visitor to the mall. She prefers a custom set of privacy

  preferences to fit her needs. Her specific settings require descriptive numerical

  parameters, as well as how the information should be shared. All of the

  businesses designated as part of the mall have the ability to aid her in locating

  product information, location, and comparisons. She agrees that they can send

  her ads (*push* services) as long as she can request (*pull* services) information on

  products. If she ignores an incoming ad, that business can no longer send her

  another ad unless she makes a request or purchase over the duration of her visit to

  the mall. She prefers that no information be shared with other entities.

In terms of setting these preferences we can assume that the fee and bonus/reward point options, defined as high and low level protections, are relatively simple to manage and may be sufficient for most users. But Elinor's medium level of privacy highlights the complexity of the UCM, in that it still requires a fair amount of user input. However, the usage scenario provides an alternative to the UCM by encapsulating an area of many businesses that can be managed with one set of privacy preferences. The UCM does not allow that type of flexibility. For example, Figure 4.3 illustrates that shopping is managed under one heading. That could encompass a broad number of businesses that are vaguely categorized under that heading. On the other hand, if provided with privacy options for each "shopping" business, the number of preferences to be set may overwhelm the user. Another possibility is that the mall would provide shoppers with a mobile device while using their service. This could eliminate the need to set preferences for low and high levels. For instance, the units would be partially preprogrammed.

5.2 Smartlists

Activities repeated on a regular basis are common. Therefore smartlist capabilities should be incorporated in the UCM as an added value for users that want tailored services without the inconvenience factor of managing individual settings. Let's assume, for example, that Elinor finds time to grocery shop during her shopping visit. The LBS system aids her in selecting products. During payment her mobile device detects the list of products she has just purchased and provides an option to save the information as a smartlist for future visits. Over time several smartlists (camping, holidays, etc.) will increase the convenience factor of grocery shopping. Furthermore, since many grocery

stores may use the same operating system, she could do her grocery shopping just about

anywhere. In fact, her smartlist could be pre-packed for pickup or delivery.

This partial evaluation exposes and addresses some of the usability issues presented in

the UCM. Chapter 6 will provide a comprehensive evaluation of the strengths and

weaknesses of the UCM.

CHAPTER 6

Evaluation

The aim of this evaluation is to find possible solutions for the UCM implementation

and to determine if any actually exist. In section 1.2 I presented the problem definition,

which this thesis has attempted to examine, in the form of the following objectives:

- Research components of LBS and the technological feasibility of implementing

  the proposed model.

- Develop a comprehensive privacy preference framework that supports primary

  LBS contexts and addresses ownership of personal information.

- Develop input controls to express privacy preferences. For example, at what

  distance do I want to be located and under what conditions?

- Implement the system on resource constrained (size, weight, memory, etc.)

  devices.

- Secure the exchange of personal information through access controls (e.g., user

  name/password). The aspects of this objective will be evaluated from a user-side

  perspective.

6.1 Framework

The framework took into consideration many of the possible interactions where

private information would flow. The four access points (LBS server, clients of LBS

server, communication list, public safety) designed to handle any type of service,

including future services, support most LBS components. They include the following interactions:

1) *Business to User:* Privacy preferences need to be managed by the primary LBS providers (business) and the user.

2) *Business to Business:* Privacy preferences need to be managed by the primary LBS providers and their business clients. The business clients need to adhere to the terms of the business/user relationship.

3) *User to Contact:* Privacy preferences need to be managed between the user, server, and the users' personal contacts.

4) *User to Requirement:* The E911 initiative (requirement) needs to be stated and privacy preferences for other emergency services need to be managed by the user.

6.2 Managing Data: Industry vs. User

While managing and implementing the UCM from an industry perspective is largely a concern of technological feasibility, from a user perspective, usability and effectiveness factors are significant concerns.

6.2.1 Industry Environment for Managing Data

The business side of management for various users types and needs for multifaceted services are complex in several aspects. A key challenge in developing the framework and input tools for the UCM was that different kinds of attributes and preferences are relevant to different applications and user types.

The proposed privacy preference layout does not consider all content and processing aspects of managing privacy. The business provider, for example, must consider that data sets are variable rather than constant and may require frequent updating. The problem with detailed content settings that frequently change is that they become more difficult for a user and business to manage. With current technology the ability to process instantaneous user profile updates has not yet been obtained. Even if daily results could be obtained, such a time lapse would deem many services useless. A secondary problem for semi prompt input would be the monetary cost involved of managing dynamic contracts. To absorb additional managing costs users and external businesses would likely have to incur them. Developing an adequate privacy preference layout during the initial stages that could be managed under all user instances may be unobtainable or inappropriate at this time. Instead, the industry may need to work toward adopting a simplified version of this model until adequate technology advancements are obtained.

6.2.1.1 Database Management Systems

Additional work needs to be done in developing techniques to provide both effective and efficient database support for LBS. Every time a user changes his preference settings the request is directed to some sort of Database Management System (DBMS). A Relational Database Management System (RDBMS) is a complex set of software programs that controls the organization, storage and retrieval of spatial data in a database (Seltzer 2005). However, unlike most conventional RDBMS that process user requests based on relatively simple data types such as characters and numeric data sets, the DBMS

48

for LBS needs to deal with continuously moving objects. The large volumes of complex

data that represent spatio-temporal content in LBS present a constant challenge to system

designers. Managing and processing spatio-temporal data is an expensive and time-

consuming process. A recently developed DBMS facilitates some of the challenges in

managing user-defined data types and functions. This new type of DBMS, known as the

Object Relational Database system (ORDBMS), enables software developers to integrate

multiple data types and methods in the same database (Ravada 2006). This technique

may be more effective and efficient than the other DBMS, but further research in LBS

environments is critical before the UCM can be fully implemented.

6.2.1.2 Connectivity

Ubiquitous computation is the result of integrating embedded computing everywhere

into the environment. Transporting data seamlessly in a ubiquitous environment would

enable users to interact with information-processing devices more naturally and casually

than they currently do, and in whatever location or circumstance they find themselves

(Koichi, Nakamura, and Kobota 2006). One of the challenges for researches is to

develop high-precision location technologies that operate over a wide area, both indoors

and outdoors. For example, GPS technologies do not work well indoors or "urban

canyons" where buildings obstruct a clear field of view between GPS satellite and

receiver. In addition, applications and user requests may require greater accuracy than a

typical GPS receiver can provide. Integrating a combination of developing technologies

is critical. One such approach for collecting data is sensor technology. The

developments of sensor networking technology enable location-based applications to

collect data through the deployment of an array of sensing devices. However, sensor technology has similar privacy risks that exist as outlined in this thesis.

6.2.1.3 Managing "Shadow" LBS

Consider applications that target subjects who don't have the ability to control privacy elements. The privacy concern arises when a subject doesn't actually own the device. Many companies keep tabs on employees for a variety of reasons. Although employer intentions may be well intended, privacy implications arise for several understandable reasons. Secondary devices such as corporate cellular phones or external GPS units are embedded in mobile entities serve as beacons/sensors, whereby data is transferred to monitoring stations. Such approaches also do not address the risks that an individual may circumvent the server and directly collect data from the location tracking system without the subject knowing. Since these devices are individually or business owned but collect data on external subjects rather than on themselves, they serve as "shadow LBS." Imposing this sort of surveillance is disturbing in some instances and may be a question of business ethics, morality, and legality. This also exposes the fact that the UCM would not be a complete control mechanism for this large sector of LBS. I suspect that the layout and type of input tools would look significantly different than what has been proposed here. For example, a fleet management company may want to control numerical measures such as vehicle speed, temperature, and weight.

6.2.2 User Environment for Managing Data

The user-side of management for various users types and needs for multifaceted services are complex in several aspects. A key challenge in developing the input tools for

the UCM was that different kinds of attributes and preferences are relevant to different applications and user types. One of the risks involved with developing extensive privacy controls is usability. Users may be reluctant to use them due to their complexities. Understanding control mechanisms require a user to have an adequate level of knowledge. The user may need to invest a fair amount of time to learn these skills. Maintaining privacy preferences is also time consuming. If a user is incapable or unwilling to managing privacy controls, privacy may be compromised.

6.2.2.1 Input Controls

The idea was to use as few tools as possible in an efficient manner to address user needs, i.e., simplify the system. The input control tools presented in the UCM appear to serve their purpose from a functional perspective in some instances and not so well in other instances. In terms of providing low and high-level privacy options, most users should find them sufficient and relatively simple to manage. However, clearly the UCM is fairly complex for users to manage dynamic (medium-level) privacy preferences. The following evaluation of the input tools brought forth some new ideas. Surrogate methods to manage privacy will be suggested as possible replacement components.

The servers of LBS and their business clients have the opportunity to retain location records for a period of time (Figure 4.2 and 4.3). However, the elimination of the "retaining location" control mechanism from the UCM would simplify the usability of the system while retaining privacy. Retaining information for any longer than necessary to process a user request is redundant and inefficient. Once the information has been used for a specific *push* or *pull* service, for example, the data should be disposed of.

51

Consider Apple's DRM (Digital Rights Management) technology as a good example of how data can be used for intended purposes (Akamai Technologies, Inc. 2005). If Apple can specify that an iTunes song can be rendered a limited number of times from a single device, then a LBS server should be able to specify that a users location can only be used once for a specific purpose. Once the data has been used for its intended purpose and purged from the system, privacy concerns over data mining and warehousing significantly subside. As a result of ensuring that data is only used once, the user could then control user/server interactions through distance parameters.

Navigating to and defining numerical measures for several general LBS topics is relatively straightforward (Figure 4.3). The user, in this example, activates "shopping" and proceeds to define the distance parameters in a few simple steps. One problem is that the topic may encompass a broad range of "shopping" services that the user may or may not be interested in. By accommodating the user with specific shopping preferences, the user's capacity to manage those preferences may be overwhelming. Furthermore, all applications have not been considered. Because applications vary and preferences may need to reflect this, what has been proposed is less than optimal. As application development broadens, appropriate control tools will become more apparent. Regardless of which types of applications are developed, distance and time are essential elements to protecting privacy as they relate to location.

The options illustrated in Figure 4.3 for *push* services appear to be functional since these service providers, by nature, need to broadly solicit their customers. However, they may not be appropriate from a users perspective since they have a tendency to alienate or

even embarrass users. The distance mechanism is also problematic. Consider a scenario

when a user driving alongside a strip mall for several blocks and receives an excessive

number of solicitations even though the distance parameter is set to cover a relatively

small area. If the user decreases the value any further the net results may prove to be few

and therefore useless. When a user is walking, a useful way of receiving *push* services

would be to set the distance parameter to zero. In this case a user would expect to receive

a solicitation only when entering an establishment.

Push services are potentially obtrusive in many instances. To envision, in the

foreseeable future, a society in which many providers of services and goods will solicit

countless LBS subscribers is not difficult. Serious debates on how to manage *push*

services are ongoing and no clear approach has been entirely acceptable, including what

has been proposed here. A partial solution includes incorporating a notice of financial

incentive to receive such services. This incentive could be stated in the menu prior to

use.

The ability of *push* services to establish a relationship with a user however is not

necessarily limited by distance parameters or financial incentives. *Push* services could be

advertised through a number of creative methods (billboard, newspaper, online, radio,

etc.) and turned into *pull* services. An advertisement, for example, may state that users

can access a Starbucks coupon by sending "coffee" as a text message and receive a

coupon code number like 123344. Notice that asking them to send you something does

not alienate customers like *push* services do.

Managing communication lists is not a new endeavor. The "friends" list as illustrated in Figure 4.4 provides a few additional options such as time and distance parameters. A certain level of concern for privacy may present itself if access privileges are applied for unintended purposes. When a user grants access privileges to a contact they must be trusted. Levels of trust could be partially controlled through distance parameters. For example, a highly trusted contact may access the location of a user by reducing the distance from one mile to 100 feet. Activating or deactivating "friends" as a group is probably not appropriate. An alternative method would be to provide an activate/ inactivate option for each friend. Furthermore, those users not interested in such detailed preferences, as time and distance parameters, could bypass that option. Users that falsify identity and numerical components also compromise privacy. Suppose that a user manipulates name/phone number combinations to hide or mislead information that contacts receive.

The public safety menu illustrated in Figure 4.6 serves useful purposes by stating the required E911 initiative and providing alternative emergency options in a clear and concise manner. As technology develops, traffic alerts, for example, could be managed through a smartphone but broadcasted through an automobiles sound/navigation system whereby alternate routes would be provided.

6.3 Hardware Resource Considerations

Mobile device developers are pressured by consumer demands to design more highly functional devices. This becomes increasingly challenging because of resource-constrained (i.e., physical and environmental) factors. As a result, physical constraints

(such as screen size, keypad, and graphical and textual elements) and environmental constraints (such as limited memory, central processing unit (CPU) power, and bandwidth) must be considered when developing mobile devices.

6.3.1 Physical Constraints

The small screens and simplified keypads that most smartphones necessitate present usability issues. For example, consider the challenges of different smartphone screen sizes. The data transmitted to user interfaces is displayed differently according to screen size and shape (Figure 6.1). Elements must be properly sized to meet high-level visual guidelines. As a result, the user will need to do more navigating on restrictive screens.
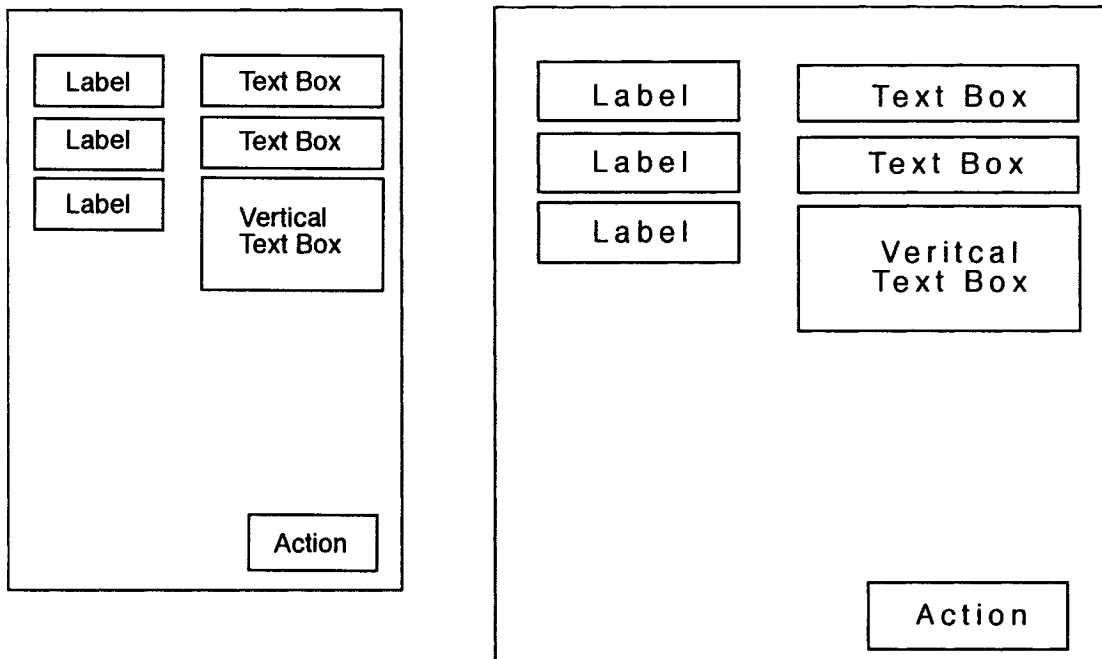

Figure 6.1: Identical elements dynamically placed to fit different screen sizes

Considering the limited input capabilities of smartphones, the ability for users to access and set privacy preferences without complicated menu selection or browsing has become increasingly important.

The size of the proposed conceptual smartphone (Figure 4.5) in the UCM may be sufficient because the device can be defined as a hand-held device. The screen, however, may not be because the device is compromised by the design. For example, a so-called "flip phone" could provide two surfaces: a maximized screen on the flip side and the control mechanisms on the other.

An evaluation of the navigational and data input tools indicates that they are cumbersome in some aspects and may deter the user from defining preferences. For example, the scroll wheel requires a user to concentrate on a continuously moving display. One idea to resolve this issue would be to code a button to navigate between windows. The potentially large data sets, however, may require a relatively large number of windows to navigate through. This is time consuming and confusing to the user. Furthermore, mobile activities such as walking and driving must be presumed. Therefore, the additional amount of concentration required during these activities may result in elevated stress levels for users. Also, the alphanumeric keypad (not illustrated) is inherently inefficient for data input. The time-consuming effort requires a user to depress one button at a time, which represents several alpha characters.

Advanced voice recognition technology is in its infancy but already provides an alternative to restrictive keypads. Hands-free Bluetooth technology is the primary source for wireless voice/hearing devices. This technology could also be used for navigation

and data modifications. For example, consider the difficulty a user would have to manually define when, where, and under which circumstances (Figure 4.4) each of his friends were allowed to contact him. Instead of navigating through several options (e.g., communication list—friends—name—address—active—time—etc.), the user could make a voice command to access, modify, etc., desired attributes. However, voice input is susceptible to security breaches and may only be appropriate for some applications. Privacy sensitive information such as social security, phone, and credit card numbers can be stolen by eavesdropping. An alternative to manual data input could be to set preferences on a computer and then transfer the data to the device. This assumes that users wouldn't have a great need to modify preferences on the fly.

6.3.2 Environmental Constraints

While physical components are approached from a structural perspective, environmental components are generally approached from a functional perspective. Understanding environmental factors will help to understand the impact they have on interface design.

Memory, processing, and bandwidth components that make a device function require large amounts of energy. Energy demands also increase as a function of screen size, number of colors, and resolution. Today, most smartphones are powered by lithium-ion (*Li-ion*) or nickel-metal hydride (*NiMH*) battery packs. Fuel cells and proton polymer batteries are in research and development and have been shown to be promising new technologies. In addition, or alternatively, developing technologies to reduce the power

consumption of smartphones instead of increasing their energy capacity may be easier for developers to attain.

The text displayed in the UCM consumes low levels of energy, but the color-coded buttons that display active/inactive features do not conserve energy. Cartographic icons or symbols are more efficient methods of displaying most data. Furthermore, color-blinded users may have difficulty distinguishing colors. However, consumer demands for multi-color screens that support video inputs must be taken into consideration.

Designing these devices to process applications efficiently in conjunction with data storage (such as dynamic privacy preferences) is a very difficult task. As the data load increases, the ability to process that data weakens to a point that may render LBS too ineffective for most uses. As the complexities of LBS applications grow, the functionality of the system will be further strained, especially during multi-tasking. Similar problems existed with the conversion from desktop to notebook computers. Today, desktop computers still have the capacity to process information more efficiently than notebooks, but not by much. When technological innovations allow engineers to design smartphones at that more efficient level, implementation will be more attainable. Although some of the better smartphones do feature adequate memory capacity and processing power, full LBS implementation is not likely unless a large portion of the population is able to afford them.

Connection speeds (bandwidth) to the wireless Internet are relatively slow for smartphones. As a result, most smartphones do not have the capacity to move large data sets from server-side systems. Connection reliability is also inconsistent.

58

Technical constraints such as a multitude of platforms, operating systems, programming languages, and protocols, for mobile devices are other concerns to consider for full LBS implementation. Some of these interoperability challenges can by reduced by standardizing LBS. Efforts by the Location Interoperability Forum (LIF), MAGIC Services Forum, and Open GIS Consortium (OGC) have recently emerged as key players.

6.4 User-side Security

The UCM presents a few user-side security issues. The dynamic nature of user-controlled privacy preferences requires the user to accept responsibility of user-defined settings under the stated terms of the service. Since the service provider will offer several services, several contracts describing how the data could be managed should be expected. Once a user accepts the terms of a contract a certificate or user name/password combination must be created to verify a proof of identity. Although the UCM does not provide an example of how and when the user would express his identity, it does however provide tools to make a choice to the conditions of a contract. In the above scenario, for example, when Elinor enters the grocery store with her smartlist she is alerted by the device whereby the contract is displayed. She enters her user name/password and simply checks the "accept" box agreeing to the terms of the contract. The UCM does not address if users would need to enter a user name/password for services used multiple times. The problem presents itself when a user alters his settings and a new contract is initiated. A likely solution would be to accept the terms of the contract only once, even if privacy preferences are altered. Proof of user name/password would continue to be required.

It is also important to remember that LBS providers and users have agreements with the wireless network carriers. Important steps must continue to be taken to ensure that data be kept private, secure, and safe.

6.5 Policy Considerations

This subsection explores other various aspects of implementing such a model. The following aspects could better facilitate adoption of the UCM when dynamically coupled with user needs.

6.5.1 Price Levels

A multitude of service plans and rates should be expected since customers have differing needs and expectations. Putting a price on privacy, however, may discriminate against lower-income subscribers. For example, should users receive a discounted rate on their service plans if they choose to receive *push* services? This is potentially an incentive for the provider but may not be for the user. In theory, the client of the server is paying (subsidizing) the server for access to the user. As a result of the revenue generated by this arrangement, LBS could offer a reduced service rate to the user. The user may benefit in terms of monetary cost, but not necessarily in terms of privacy protection. If subscriptions increase as expected (and therefore profits), potential rate reductions in pricing plans could occur. On the flipside one could argue that compromising privacy will reduce LBS growth rates. Furthermore, *push* services have a tendency to be intrusive and the nuisance factor has the potential to grow exponentially as LBS use increases. In short, subscribers who gravitate towards the lowest prices receive a lower quality service while compromising privacy.

6.5.2 Ethics

An appropriate framework of ethics, at a practical level, should be based on choice. The underlying ideology of choice is fairly simple: a choice is morally correct, if it puts minimal constraints on other peoples' ability to make choices for themselves. The UCM reflects strongly the underlying ethic of choice, as demonstrated, by offering users clear, conspicuous choices. Informed choices are made if:

- The user is capable and willing to make a choice.

- The user knows that a choice can be made.

- The user knows what the consequences of a choice are.

6.5.3 Model Uncertainty

Definitive answers to these aspects, as well as several areas of concern already presented in the evaluation, cannot be validated until future research is conducted. The next step for implementation purposes will require user validation of the UCM concepts and solutions. The results from an operational prototype will further address the question of success for this type of system.

6.6 Evaluation Summary

An evaluation of the UCM offered several positive and negative insights into some of the implications of model design concepts. Benefits of the model are that a user could control most ownership issues with the proposed privacy tools by defining and modifying privacy settings, which are governed by a legal framework and contract language that rests upon the principles of individual privacy. Some of the negative aspects of the

model are that implementation may be difficult because of usability, industry adoption, and technology factors.

Although there is a concern that the UCM is not entirely capable of serving the purpose for which it was designed, progress has been made. An important aspect that was investigated (Chapters 4 & 5) was determining levels of privacy adequate for the majority of users. The multi-level privacy infrastructure may be sufficient in terms of user requirements. Recent research indicates that relatively basic privacy-enhancing tools significantly reduced privacy concerns by 87 percent of the test subjects (Hauknes 2003). The point is that a simplified model is all that may be required to resolve the bulk of privacy issues. However, users have a tendency to have a poor understanding of privacy threats (Hauknes 2003).

The most attainable and appropriate outcome may be a model that fits somewhere between multi-level control (low, medium, high) and full dynamic control (Figure 6.2). This equilibrium may provide a sufficient level of privacy to the majority of users. Over time, technology will permit more control and some sort of equilibrium will likely result.
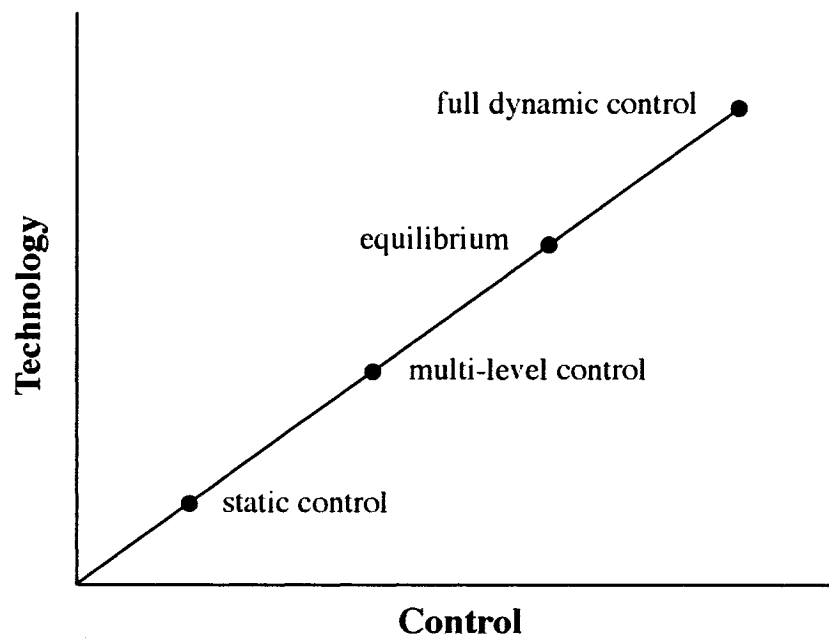
Figure 6.2: Changes in user-control are determined by technology and usability

CHAPTER 7

Conclusions

This final chapter will draw some conclusions based on the results and experiences

gained from the work with this thesis.

7.1 Thesis Conclusions

This research has been based around the user-centric framework for developing the

UCM and constitutes one of the most important steps in thoroughly protecting privacy of

LBS users. The design is dynamic in nature, allowing users the flexibility to manage

privacy preferences. However, the design is not sufficient in itself unless the overall

objectives of policy are clearly identified—which they are not. Instead, the United States

has relied more on self-regulation than legal regulation. Loosely defined laws, such as

the Foreign Intelligence Surveillance Act of 1978, resulted in government abuse of power

as demonstrated by the recent Bush administration's decision to wiretap US citizens with

supposed links to terrorism. From a privacy point of view, a clear distinction exists

between surveillance of an individual based on grounded suspicion, and surveillance of

groups based on characteristics in their personal profiles (Hauknes 2003). If the need for

increased surveillance arises on the basis of national security or public safety, the privacy

aspects must not be forgotten.

In 1975 the US Government collected an estimated 100 billion pages of information

on over 10,000 US citizens, including Martin Luther King, giving the government "an

extraordinary record and instrument of control over its citizens"(Daon 2003). The

integrity of the government's future decision-making will hinge on its ability to understand, analyze, and communicate complex information effectively, while also taking into account the individual's perspective on privacy.

By implementing this conceptual UCM and appropriate regulations, LBS and technologies can be applied while also ensuring privacy of individuals. According to Data Protection Commissioner Ann Cavoukian:

> "[GIS] systems can be designed to place the power of the [GIS] in the hands of the individual as opposed to companies or governments. Applications can be configured to give the data subject the ability to control access to his or her own data, to safeguard the integrity of their personal information and protect their identity against misappropriation" (White 2003).

Three organizations (WLIA, P3P, IETF) have made attempts to address legislative shortcomings and rapidly advancing technological innovations through self-regulation. Their analysis indicates that managing privacy needs to be implemented within a strategically developed framework based on a clear and shared vision. The primary problems with self-regulation are that regulators have no clear enforcement solutions, limited in scope, and procedures vary. Self-regulation also becomes more difficult with larger and more diverse LBS. Although a number of shortcomings have been cited, the insights gained into their frameworks were very useful. They have served as building blocks for this conceptual UCM, especially in terms of focusing on user contexts.

7.2 Project Lessons

Privacy issues are inherently important in the adoption of LBS and technologies. The transformation of the cell phone into a multimedia and location-tracking tool has raised location privacy issues even further. The fact that someone other than the individual with

the mobile device knows where that person is located and has the ability to track the individual is widely considered disconcerting. Over the past decade, rapid development of wireless and GPS technology for mobile location-determining purposes has grown and is expected to expand from E911services, telematics, and other services to becoming essential to the livelihood of most Americans. The use of LBS technology has proven to be effective, and therefore appropriate for wide spread use. However, the use of LBS technology must be applied in a manner that minimally impacts the rights of individuals.

The failure to follow the procedures of the Foreign Intelligence Surveillance Act of 1978, plus the failure to implement the Location Privacy Protection Act of 2001, and then the subsequent passage of the USA Patriot Act have systematically eroded privacy rights and have reaffirmed the need for a review and strengthening of privacy protections.

7.3 Recommendations

In conclusion, the following recommendations are made regarding the implementation and regulation of the UCM to ensure privacy.

- Consumers should receive *notice* of the information that is collected, including who is collecting data, what, how, and why data is collected, how data is being protected, and what choices are available.

- Consumers should have *access* to their shared data (the right to view or obtain a physical copy of the data without a fee) and the right to have inaccurate or incomplete data rectified.

- Consumers should have a *choice* regarding the scope of disclosure of information. A range of choices would be adjusted to reflect user-defined preferences.

Disclosure of information could not be used for unintended purposes, particularly

if the information can be used against the consumer. The consumer would have

the right of recourse in the event of unlawful processing.

- Data bank *security* must be developed and maintained in accordance with the

  provider's system. The provider must adhere strictly to stringent data security

  standards.

- Legal *enforcement* should be accomplished by the individual LBS provider and

  administrated by a separate institution to ensure uniformity and consistency.

7.4 Future Work

Although an operational prototype has not yet been developed, a proof of concept

should be developed. The P3P consortium is likely to test concepts, similar in nature to

the proposed UCM, which could yield some interesting results. These types of actions

would indicate a change of the overall trends and may address the question of success for

this type of system.

References

ABI Research. GPS IC Markets: RF and Baseband Semiconductor for A-GPS and GPS
    Equipment Solutions. 2Q 2004. Online. Internet. 2 Mar. 2005. Available:
    <www.abiresearch.com/products/market_research/GPS_IC_Markets#>.

Agre, Jonathan, et al. A Layered Architecture for Location-based Services in Wireless Ad
    Hoc Networks. 19 Nov. 2001. Online. Internet. 8 Nov. 2006. Available:
    < www.flacp.fujitsulabs.com/FLA-PCRTM01-01-LSM.pdf>.

Akamai Technologies, Inc. Monetizing Media Through Digital Rights Management.
    2005. Online. Internet. 8 Nov. 2006. Available: <www.akami.com/dl/whitepapers/
    Monetizing_Media_Assets_Whitepaper.pdf>.

Andersson, Christoffer. Mobile Positioning – Where You Want To Be! Online. Internet.
    20 Sept. 2005. Available: <wirelessdevnet.com/channels/lbs/features/mobile
    positioning.html>.

Ang, Peng. "The Role of Self-Regulation of Privacy and the Internet." Journal of
    Interactive Advertising, Volume 1, Number 2, 2001. Online. Internet. 3 Dec. 2005.
    Available: <http://www.jiad.org/vol1/no2/ang/index.htm>.

Boertien, Nicky, and Eric Middelkoop. Location Based Services. 2002. Online.
    Internet. 9 Nov. 2006. Available: <doc.telin.nl/dscgi/ds.py/Get/File23319/location_
    based_services.pdf>.

Camp, L. Jean and Carlos Osorio. Privacy Enhancing Technologies for Internet
    Commerce. 2003. Online. Internet. 30 Nov. 2005. Available: <www.ljean.com
    /files/CampOsorio.pdf>.

CCIPS (Computer Crime and Intellectual Property Section) of the Criminal Division of
    The US Department of Justice. "Communications Assistance for Law Enforcement
    Act (CALEA)." 16 Apr. 2003. Online. Internet. 15 Apr. 2004. Available:
    <www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm>.

Chang, Kang-Tsung. 2002. Introduction to Geographic Information Systems. New
    York: McGraw-Hill Companies, Inc.

Cotler, Edward and Stephen Larson. "Internet Wiretapping and Carnivore." 17 May
    2001. Online. Internet. 15 Apr. 2004. Available: <www.swiss.ai.mit.edu/6.805/
    student-papers/spring01-papers/carnivore.doc>.

Daon. Biometrics: Protecting Your Privacy and Identity. Jan. 2003. Online. Internet.

25 Apr. 2004. Available: < www.daon.com/white%20papers/whitepaper1.htm>.

EFF (Electronic Frontier Foundation). EFF Analysis of the Provisions of the USA Patriot Act. 31 Oct. 2001. Online. Internet. 4 May 2004. Available: < www.eff .org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.html>.

FCC (Federal Communication Commission). CC Docket No.94-102. 1996. Online. Internet. 10 Mar. 2004. Available: <www.911.state.tx.us/files/pdfs/resources /fcc96264.pdf>.

FCC (Federal Communication Commission). FCC Acts on Wireless Carrier and Public Safety Requests Regarding Enhanced Wireless 911 Services. 2001. Online. Internet. 17 Apr. 2004. Available: <www.fcc.gov/Bureaus/Wireless/News_Releases /2001/nrwl0127.html>.

Froomkin, Michael. "The Death of Privacy?" 2000. Online. Internet. 3 Dec. 2005. Available: <osaka.law.miami.edu/~froomkin/articles/privacy-deathof.pdf>.

Geier, Jim. "802.1X Offers Authentication and Key Management." 7 May 2002. Online. Internet. 2 May 2006. Available: < www.wi-fiplanet.com/tutorials/ article.php/1041171>.

Hassim, Yunos and Jerry Gao. Wireless Advertising. 2002. Online. Internet. 26 Oct. 2005. Available: <www.engr.sjsu.edu/~gaojerry/course/296A/wireless-add-paper2.pdf>.

Hauknes B. Christian. User-Centered Privacy Aspects in Connection with Location-Based Services. 2003. Online. Internet. 16 Jan. 2006. Available: <www.personvern .uio.no/pvpn/artikler/Hauknes_cand%20scient%20thesis.pdf>

IETF (Internet Engineering Task Force). Geographic Location/Privacy (GeoPriv) Charter. Online. Internet. 6 Apr. 2005. Available: <www.ietf.org/html.charters/ geopriv-charter.html >.

Koichi, Takasugi, Motonori Nakamura, and Minoru Kubota. Seamless Service Platform For a Ubiquitous Network Environment. Aug. 2003. Online. Internet. 8 Nov. 2006. Available: <www.ntt.co.jp/tr/0308/files/ntr200308089.pdf>.

LaMance, Jimmy, Javier DeSalas, and Jani Jarvinen. "Assisted GPS: A Low-Infrastructure Approach. " GPS World. Mar. 2002. Online. Internet. 26 Sept. 2005. Available: <www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=12287&sk = &date=&pageID=2>.

Markkula, Jouni. "Dynamic Geographic Personal Data – New Opportunity and Challenge Introduced by the Location-Aware Mobile Networks." <u>Cluster Computing</u> 4 (2001): 369-377.

Mobiledia Corp. 2004. Online. Internet. 8 May 2004. Available: <www.mobiledia.com/glossary/249.html>.

Olesen, Henning, et al. User-Centric Factors of Context Aware Services. Online. Internet. 18 Nov. 2005. Available: <www.ist-magnet.org/private/files/Dissemination/ WP1/User-centric%20factors.pdf >.

Onsrud, Harlan. Personal Information Privacy Protection within Intelligent Spatial Technology Domains. Online. Internet. 4 Oct. 2005. Available: <www.spatial.maine.edu/~onsrud/research/privacy.pdf>.

Onsrud, Harlan, et al. The Future of the Spatial Information Infrastructure. 2004. Online. Internet. 19 Feb. 2007. Available: <www.spatial.maine.edu/~onsrud/pubs/ chapter8preprint.pdf>.

OnStar. 2004. Online. Internet. 13 Apr. 2004. Available: <onstar.internetpressroom. com/pressroom.cfm >.

P3P (Platform for Privacy Preferences). Online. Internet. 3 Oct. 2005. Available: <www.w3.org/P3P/>.

Peng, Zhong-Ren and Ming-Hsiang Tsou. 2003. <u>Internet GIS.</u> New Jersey: John Wiley & Sons, Inc.

Peterson, J. A Presence-based GEOPRIV Location Object Format. 9 Sept. 2004. IETF: GEOPRIV, Internet Draft. Online. Internet. 6 Apr. 2005. Available: < www.ietf.org/internet-drafts/draft-ietf-geopriv-pidf-lo-03.txt >.

Pfoser, D. and Christian S. Jensen. Capturing the Uncertainty of Moving-Object Representations. May 1999. Online. Internet. 7 Dec. 2005. Available: <www.cs.aau.dk/~csj/Papers/Files/1999_pfoserSSD.pdf>.

Ravada, Siva. Spatial Database Services for Location-aware Applications. Online. Internet. 8 Nov. 2006. Available: <www.gisdevelopment.net/technology/lbs/techlbs 004pf.htm>.

Riley, Steve. "Mitigating the Threats of Rogue Machines—802.1X or IPsec?" 9 Aug. 2005. Online. Internet. 2 May 2006. Available: <www.microsoft.com/technet/ community/columns/secmgmt/sm0805.mspx>.

Schulzrinee, H., et al. A Document Format for Expressing Privacy Preferences for Location Information. 28 Nov. 2004. IETF: GEOPRIV, Internet Draft. Online. Internet. 7 Apr. 2005. Available: <www.ietf.org/Internet-drafts/draft-ietf-geopriv-policy-05.txt>.

Seltzer, Margo. Beyond Relational Databases. 3 Apr. 2005. Online. Internet. 8 Nov. 2006. Available: <acmqueue.com/modules.php?name=Content&pa=showpage&pid=299>.

TechTarget. 9 Jul. 2001. Online. Internet. 24 Feb. 2005. Available: <searchnetworking.techtarget.com/sDefinition/0,,sid7_gci753924,00.html>.

Tele Atlas. Real-time Traffic & Dynamic Rerouting. 3 Mar. 2003. Online. Internet. 2 Oct. 2005. Available: <www.na.teleatlas.com/pdfs/real_time_traffic.pdf>.

The Company v. The United States of America. 18 Nov. 2003. Online. Internet. 13 Apr. 2004. Available: <www.ca9.uscourts.gov/ca9/newopinions.nsf/7BD3F8D6A 62D994588256DE2005C863B/$file/0215635.pdf?openelement>.

Wagner, Matthias, et al. A Roadmap to Advanced Personalization of Mobile Services. Online. Internet. 4 Nov. 2005. Available: <www.l3s.de/~balke/paper/coopis02i.pdf >.

White, C. James. 2003. People, Not Places: A Policy Framework for Analyzing Location Privacy Issues. Spring 2003. Online. Internet. 4 Apr. 2004. Available: <www.epic.org/privacy/location/jwhitelocationprivacy.pdf>

WLIA (Wireless Location Industry Association). Draft WLIA Privacy Policy Standards. 2001. Online. Internet. 21 Mar. 2005. Available: <www.wliaonline.com/indstandar d/privacy.html>.

Yuan, Xiaowei, et al. The Structure Design of Smart Phone User Interface. 9 Nov. 2006. Available: < www.isaruid.com/download/news/1948.PDF>.