Université de Montréal

Wireless Privacy and Personalized Location-based Services: The Challenge of Translating the Legal Framework into Business Practices

Par
Eloïse Gratton

Faculté de Droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de L.L.M.,
option technologies de l'information

Août 2002

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé

Wireless Privacy and Personalized Location-based Services : The Challenge of Translating the Legal Framework into Business Practices

Présenté par :

Eloïse Gratton

a été évalué par un jury composé des personnes suivantes :

Karim Benyekhlef
Président-rapporteur

Pierre Trudel
Directrice de recherche

Daniel Poulin
Membre du jury

ABSTRACT

The proliferation of mobile communications is leading to new services based on the ability of service providers to determine, with increasing precision and through the use of location determination technologies, the geographic location of wireless devices and allow their users to receive services based on such location.

The development of location-based services introduces new privacy risks for consumers that must be addressed. The portability of wireless devices coupled with their ability to pinpoint the location of wireless users and reveal it to others could produce a system where the everyday activities and movements of these users are tracked and recorded, and where wireless users receive unanticipated messages on their device.

For this reason and in order to preserve the privacy of wireless users, a company looking to deploy a technology related to the providing of personalized location-based services ("LBS Provider") will have to analyze the privacy legal framework, coming either from legal sources--that may be in some case vague and not specific to this new context--or from the industry, and translate such framework into business practices. Such analysis may help in establishing what kind of business model and technology should be adopted and developed by LBS Providers in order to ensure the privacy of wireless users while providing this new type of service.

RÉSUMÉ

L'avancement des communications sans-fil permet l'obtention de nouveaux services basés sur l'habileté des fournisseurs de services sans-fil à déterminer avec précision, et avec l'utilisation de technologies de pistage, la localisation et position géographiquement d'appareils sans-fil. Cette habileté permet d'offrir aux utilisateurs de sans-fil de nouveaux services basés sur la localisation et la position géographique de leur appareil.

Le développement des services basés sur la localisation des utilisateurs de sans-fil soulève certains problèmes relatifs à la protection de la vie privée qui doivent être considérés. En effet, l'appareil sans-fil qui suit et enregistre les mouvements de l'utilisateur permet un système qui enregistre et entrepose tous les mouvements et activités d'un tel utilisateur ou encore qui permet l'envoi de messages non anticipés à ce dernier.

Pour ce motif et afin de protéger la vie privée des utilisateurs de sans-fil, une compagnie désirant développer ou déployer une technologie permettant d'offrir ce genre de services personalisés devra analyser l'encadrement légal touchant la protection des données personnelles--lequel est dans certains cas vague et non approprié à ce nouveau contexte--ainsi que la position de l'industrie dans ce domaine, et ce, afin d'être en mesure de traduire cet encadrement en pratiques commerciales. Cette analyse permettra d'éclairer le fournisseur de ces services sur la façon d'établir son modèle d'affaires et sur le type de technologie à développer afin d'être en mesure de remédier aux nouveaux problèmes touchant la vie privée tout en offrant ces nouveaux services aux utilisateurs de sans-fil.

KEY WORDS:

Wireless

Mobile

Location

Privacy

Personal data

Personalization

Profiling

Location-based services

Location data

Tracking technology

Business Practices

MOTS CLÉS:

Sans-fil

Mobile

Localisation

Vie privée

Donnée(s) personnelle(s)

Personnalisation

Profilage

Services basés sur la localisation

Données de localisation

Technologie de pistage

Pratiques commerciales

TABLE OF CONTENTS

LIST OF SCHEDULES

LIST OF FIGURES

GLOSSARY OF ABREVIATIONS, ACRONYMS AND TERMS

Aggregate	Data that is combined together without releasing PII.
ASP	(Adjunct Service Point) An intelligent-network feature that resides at the intelligent peripheral equipment and responds to service logic interpreter requests for service processing.
Base station	A land station in the land mobile service. For example, in cellular and personal communications uses, each cell has its own base station; each base station is interconnected with other base stations and with the public switch network.
Carrier	A government-regulated private company offering telecommunications services or communications facilities to the general public on a non-discriminatory basis under operating rules mandated by the appropriate state and/or federal regulatory authority.
CDT	(Center for Democracy and Technology) A non-profit organization dedicated to advancing individual liberties and democratic values in new communications media.
Cell site	The location where the wireless antenna and network communications equipment is placed.
Content provider	In the context of the present paper, a company looking to send personalized content or advertising to wireless users based on such users' geographical locations to make the content relevant.
Cookie	A short file put on the system by a web page that includes information about usage and facilitates the current interaction. For example, it may include the information that the user has logged into a passworded area in the current session that is saved as a cookie to alleviate a second password check. There are many uses for cookies; they may be erased at the end of a session or retained until the next session, and they may be encrypted or in plain text.
CPNI	(Customer Proprietary Network Information) The carrier's data about a specific customer's service and usage which includes the location, duration and frequency of phone calls. The FCC restricts CPNI use in marketing.
CTIA	(Cellular Telecommunications & Internet Association) Previously working under the name of Cellular Telecommunications Industry Association, a trade group representing cellular, PCS and enhanced specialized mobile radio carriers.

Demographic data	Data about an individual's characteristics such as gender, age, and income.
Digital	Any type of information that can be outputted, transmitted and interpreted as individual bits of binary information, using electrical or electromagnetic signals that can be modulated to convey their specific content.
DMA	(Direct Marketing Association) The oldest (since 1917) trade association for users and suppliers in the direct, database and interactive marketing field.
E-mail	(Electronic Mail) Messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses.
Encryption	The discipline which embodies principles, means, and methods for the undetected modification or prevention of unauthorized use. Cryptography is limited to the transformation of information using parameters or associated key management.
EPIC	(Electronic Privacy Information Center) A non-profit research and educational organization that examines the privacy and civil liberties implications of emerging technologies.
FCC	(Federal Communications Commission) The FCC is an independent United States government agency, directly responsible to Congress, established by the Communications Act of 1934, and charged with regulating interstate and international communications by radio, television, wire, satellite and cable.
Geographically tagged PII	PII that is linked to location data or to a particular location through use of location-based services.
GPS	(Global Positioning System) A series of 24 geo-synchronous satellites that continuously transmit their position. Used in personal tracking, navigation and automatic vehicle location technologies.
GSM	Global System for Mobile Communications, an open, non-proprietary system that provides international roaming capability.
Internet	An unregulated, global confederation of computer networks linked through regional, private business, and educational networks. An estimated 20 million people in more than 50 countries use the Internet daily. The internet began in 1969 as an attempt by the U.S. Defense Department to link universities to Pentagon researchers, while also serving the national security purpose of spreading crucial computing tasks throughout a wide

	geographic area. Today most of the Internet's growth is in the commercial sector.
LBS Provider	In the context of the present paper, a company providing or looking to provide location-based services to wireless users.
Location-based advertising	The delivery of advertisements, coupons, and other forms of promotional and transaction-driven content to wireless devices based on their geographical position.
Location-based services	New services based on the ability of service providers to determine, with increasing precision, the geographic location of the accessing wireless devices that allow wireless users to receive services based on such geographic location, position, or known presence.
Location data	(or location information) Data relating to the geographical position of a wireless device and derived from a tracking or location determination technology.
Location data (historical)	The location data relating to the wireless user's historical geographic movement over time that is recorded, collected, and stored in order to provide such user with personalization, based on his Dynamic Profile.
Location data (real-time)	The location data of a wireless user's device at a specific time in order to send such user with a push message that appears to be in the right location, at the right time to make such a message relevant.
M-commerce	(or mobile-commerce) The facilitation of monetary transactions including purchases of products or services using wireless devices like digital wireless phone or a PDA that accesses the Internet using a wireless data connection or a private network.
MMA	(Mobile Marketing Association) Previously working under the name of the Wireless Advertising Association, a group of carriers, advertising agencies, device manufacturers, wireless advertising providers, and related, which is involved in establishing guidelines for any wireless advertising medium.
Network	A combination of transmission facilities and switching capacity that allows users to communicate with other users of linked facilities. Examples: local exchange telephone networks, cellular wireless networks, cable television networks, and private facility-based networks.
Non-PII	Information not uniquely and reliably linked to a particular person, including--but not limited to--activity on a wireless

	network such as anonymous location or aggregate location statistics. Information identifying the geographic origin of one or more signals is considered Non-PII, provided that information is not linked to or associated with any PII.
Opt-in (Confirmed)	The process of verifying a wireless user's permission each time the service is provided either through separate contact at that time or through a process of confirmation that permission has been expressly granted for a period of specific and limited duration made clearly known to the user at the time such user granted permission.
Opt-in (Standard)	A process that requires active choice on the part of the wireless user to express permission or consent for each individual use of the device or application.
Opt-out	A process by which the wireless user takes action to withdraw or deny permission whether or not he has previously opted in.
PCS	(Personal Communications Services) A two-way, digital voice, messaging, and data service designed as the second generation of cellular.
PDA	(Personal Digital Assistant) A portable computing device capable of transmitting data.
Personalization	(or profiling, as the case may be) The use of technology and customer information to tailor interactions between a business and an individual customer to fit that customer's stated or perceived needs, in order to make the interaction efficient and satisfying for both parties and to build a relationship that encourages loyalty.
Petition	The petition from CTIA requesting the FCC in November 2000 to begin a rule-making procedure for tracking the location of wireless-device users. It has asked the FCC to adopt rules that would prohibit the collection of location data from wireless phones users unless they have opted in to such collection.
PII	(Personally Identifiable Data) Information that can be used to identify a person uniquely and reliably, including but not limited to name, address, telephone number, e-mail address and account or other personal identification number, as well as any accompanying data linked to the identity of that person.
Pinpoint Tool	For the purpose of this paper, a comprehensive software solution for precision targeting, efficient planning, and real-time reporting, which interface allows content providers to manage their wireless campaigns from start to finish, enabling content creation and

	detailed scheduling and rotations, message caps and frequency specifications. Furthermore, content providers using this tool can monitor real-time statistics, conduct post-campaign analysis and track trends and response.
Profile (Dynamic)	A wireless user's profile that is based on his wireless device's location data that is collected over time and based on the wireless user's location habits, patterns, lifestyle, and preferences in order to provide such user with personalized services.
Profile (Static)	A wireless user's profile based on a combination of demographic and psychographic data related to such user in order to provide such user with personalized services.
Profile Manager	For the purpose of this paper, a tool incorporated in a web page associated with the user's profile (through his carrier's website) enabling such user, who has agreed to receive location-based services, to provide demographic and psychographic information. This tool would also cover all of the consent issues like the time, location, type, and frequency of messages he wishes to receive. Such tool would also enable the user to go back to his profile and update any profile data at any time and also have the capability of requesting that all of this profile information be deleted.
Push	Information, sometimes called alerts, sent to devices as short bursts of text, generally 160 characters or less. Privacy and consumer rights issues surround "push" advertising, since it is the model that is most likely to be intrusive considering it may be unsolicited.
Pull	The process of actively seeking and requesting wireless data using a wireless device. This process is similar to browsing for information on the wired web.
Real time	Usually used to describe situations when two or more people are interacting via their keyboards on the computer in real time, versus delayed back-and-forth communication, such as with e-mail.
Satellite	A radio relay station that orbits the earth. A complete satellite communications system also includes earth stations that communicate with each other via the satellite. The satellite receives a signal transmitted by an originating earth station and retransmits that signal to the destination earth station(s). Satellites are used to transmit telephone, television, and data signals originated by carriers, broadcasters, etc.
Service provider	For the purpose of this paper, a carrier, a LBS Provider, or a third party providing a wireless application, as the case may be.

SMS	(also known as "Short Message Text Service" or "alerts") Short bursts of text, generally 160 characters or less, sent to wireless devices. Messaging is synonymous with text paging, e-mail, or short messages received on alpha-numeric pagers and other wireless devices.
Spam	Flooding message boards, newsgroups, mailing lists, or electronic mailboxes with off-topic messages (usually ads or promotions) or deliberate disruptions or an inappropriate attempt to use a mailing list or other networked communications facility as if it was a broadcast medium by sending the same message to a large number of people who did not ask for it.
Subscriber	Any customer who has contracted for wireless services or applications from a carrier. The subscriber may be different from the actual user of the device being located.
TDMA	(Time Division Multiple Access) A digital transmission technology that allows a number of users to access a single radio-frequency (RF) channel without interference by allocating unique time slots to each user within each channel.
Telecommunications	Any transmission, emission or reception of signs, signals, writing, images, sounds, or intelligence of any nature by wire, radio, optical or other electromagnetic systems.
Terminal	A device capable of sending, receiving, or sending and receiving information over a communications channel.
Tracking technology	(or location determination technology, as the case may be) Pinpoint technologies that are either (i) network-based solutions that rely on accessing information in a carrier's home location register to locate the mobile device or (ii) handset-based solutions that rely on Global Positioning System ("GPS") information derived from a GPS chip in the handset and reported to the provider over the wireless network. Such technology would allow an organization to know the exact location of a wireless device.
WAP	(Wireless Application Protocol) An application environment and set of communication protocols for wireless devices designed to enable manufacturer-, vendor-, and technology-independent access to the Internet and advanced telephony services.
Web	The visual component of the Internet. Created with HTML language, web pages can include text, pictures, sound clips, video, links for downloading software, and much more. The Web is only one component of the Internet, although the terms are often (and mistakenly) interchanged.

Wireless	(or mobile) Use of the radio frequency (RF) spectrum for transmitting and receiving voice, data, and video signals for communications.
Wireless Internet	A radio frequency (RF)-based service that provides access to the Internet.
Wireless Push advertising	Any content sent by or on behalf of advertisers and marketers to a wireless device at any time other than when the wireless user requests it. Push Messaging includes audio, SMS messages, e-mail, multimedia messaging, cell broadcast, picture messages, surveys, or any other pushed advertising or content.
Wireless Pull advertising	Any advertising content sent to the wireless user upon request shortly thereafter on a one-time basis. For example, when a customer requests the local weather from a WAP-capable browser, the content of the response, including any related advertising, is Pull Messaging.
Wireless spam	Push Messaging or spam related to the wireless user's location or device that is sent without such user's prior permission.
Wireless user	A physical person using a wireless device.
WLIA	(Wireless Location Industry Association) The voice of the emerging wireless location industry and its member companies that provide hardware, software, services and other products related to the new ability to locate the precise origin of wireless radio signals that add consumer value based on the geographic locations of wireless device users.

ACKNOWLEDGEMENTS

I wish to express sincere appreciation to Professor Pierre Trudel under whose supervision, guidance, advice and encouragement this work was performed.

Many thanks go to the co-founders of Profilium Inc. for opening up entire new worlds to explore. Their ideas are the ultimate inspiration for this work.

I also thank my family and Stephan for their enduring support.

Introduction

The proliferation of mobile communications is leading to new services based on the ability of service providers to determine, with increasing precision, the geographic location of the accessing wireless device which allows wireless users to receive services based on their geographic location, position, or known presence (hereinafter **location-based services**). This is achieved through the use of the location data of the wireless user's device derived from location determination technologies, which are either network-based solutions or handset-based solutions. Network-based solutions are relying on accessing information in a carrier's home location register or other sources to locate the wireless device. Handset-based solutions rely on Global Positioning System (hereinafter **GPS**) data derived from a GPS receiver chip installed in a wireless device and then reported to the provider over the wireless network.

Using these tracking location determination technologies, companies providing location-based services to wireless users (hereinafter **LBS Providers**) can potentially create and target personalized content to a very specific consumer group or even to individual consumers, virtually anywhere, at any time based on the geographic position of the wireless user. Also, localization extends personalization and the capture, use, and analysis of the wireless user's location data, particularly when it is cross-referenced with other data sources, could most likely be a powerful new marketing analysis tool for businesses.[1] Such tool would enable content providers to customize and deliver highly personalized content and advertising to wireless users (such as entertainment information, traffic reports, maps and directions, interactive games), based on the geographic location of such users, and on a *push* basis.[2]

The development of location-based services, for all its convenience and usefulness, introduces new and heightened privacy risks for consumers that must be addressed. The portability of wireless devices and the ubiquity of their applications coupled with their ability to pinpoint the location of wireless users and reveal it to others could produce a system whereby the everyday activities and movements of these users are tracked and recorded. Furthermore such system would enable wireless users to receive unanticipated messages on their wireless device, commonly referred to as *wireless*

---

1 Arabella Hallawell, *Beyond the Headlines: Privacy Issues and the Enterprise*, GARTNER INC., May 4, 2001. (The footnotes follow *The Bluebook, A Uniform System of Citation*, 17th Edition. Please note that, in order to facilitate the reading of this paper, a derogation to the rules of such system is made when referencing inter footnotes.)

spam, and generally considered a form of privacy violation.

A LBS Provider looking to deploy a technology that would enable the providing of location-based services as of today is more likely to be looking to deploy globally or at least in more than one country. For this reason, such LBS Provider will have to comply with the laws related to the protection of personal or location data and to the protection against spam, wherever it wishes to deploy such new service.

In view of the potential privacy issues resulting from location-based services, a LBS Provider looking to deploy its technology in North America and in Europe will analyze the relevant North American and European legal framework. These laws and regulations seem to be providing a general privacy framework, but they are in some cases vague and are not specific to this new context. More specifically, these laws and regulations do not specify to LBS Providers how to conduct their businesses and what type of technology they should be developing in order to ensure the privacy of wireless users, while providing these new types of services. They also do not specify to LBS Providers how to obtain meaningful consent from the wireless user prior to pushing location-based messages to his device, how to collect quality data and develop the appropriate security system while also enabling wireless users to have access to the collected data.

For this reason, an analysis of the present privacy rules, but also of recent initiatives coming either from legal sources (like the introduction of new bills) or from the industry side, that are specific to the new privacy issues surrounding location-based services also need to be made.

On the legal side, the European Commission issued on July 12, 2000 a proposed directive for an amendment to the *EC Directive 97/66/EC*,[3] in order to update provisions to cope with technology evolution, such as the move from fixed to wireless communications and from voice to data. This proposal was accepted on November 13, 2001 by the European Parliament with certain amendments (hereinafter the **2000 EC Proposal**).[4] It introduces safeguards for wireless users with regards to

---

2 Please refer to Subsection 3.2.3.1 for details relating to the "push" and the "pull" model.

3 Commission of the European Communities, *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* (presented to the Commission – Legislation under preparation), COM (2000) 385 Final, 2000/0189 (COD), Brussels (July 12, 2000).

4 European Union, *Proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of*

location-based services,[5] and gives users the right to refuse unsolicited communications for direct marketing purposes, and extends to cover all forms of electronic communications.[6] The 2000 EC Proposal was eventually amended in January 2002[7] and these changes translated into amendments to be incorporated in the *EC Directive 97/66/EC* in April 2002.[8]

In North America, U.S. bills introduced in 2001 like the *Wireless Privacy Protection Act*,[9] the *Location Privacy Protection Act*[10] and the *Wireless Telephone Spam Protection Act*[11] seem to have addressed some of the privacy issues resulting from this new type of services.

On the industry side, the U.S. Federal Communications Commission's[12] (hereinafter the **FCC**) E-911 mandate[13] may accelerate consumer demand for location-based services. Such mandate requires carriers to either begin selling handsets that are equipped with locator devices or to upgrade their networks so that a caller's location can be pinpointed by signal strength. In order to address the privacy concerns regarding wireless privacy, the U.S. Federal Trade Commission[14] (hereinafter the **FTC**) began exploring wireless privacy issues at a *Public Workshop on Emerging Technologies and*

---

privacy in the electronic communications sector, Bulletin EU 11-2001, Information Society 7/11, November 13, 2001. http://europa.eu.int/abc/doc/off/bull/en/200111/p103104.htm (Last accessed on July 8, 2002)

5 Article 9, Commission of the European Communities, *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* (presented to the Commission – Legislation under preparation), COM (2000) 385 Final, 2000/0189 (COD), Brussels (July 12, 2000).

6 *Id.* Article 13.

7 Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

8 European Parliament, *II Recommendation for second reading on the Council common position for adopting a European Parliament and Council directive concerning the processing of personaln data and the protection of privacy in the electronic communications sector*, Committee on Citizen's Freedoms and Rights, Justice and Home Affairs, Final (April 22, 2002).

9 The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

10 The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

11 The Wireless Telephone Spam Protection Act, H. R. 113, 107th Congress, 1st Session (2001).

12 The FCC is an independent United States government agency, directly responsible to Congress and established by the Communications Act of 1934 and charged with regulating interstate and international communications by radio, television, wire, satellite and cable. http://www.fcc.gov/ (Last accessed on July 8, 2002)

13 http://www.fcc.gov/911/enhanced/ (Last accessed on July 8, 2002)

14 The Federal Trade Commission enforces a variety of federal antitrust and consumer protection laws in the United States. http://www.ftc.gov/ (Last accessed on July 8, 2002)

Consumers Issues in December of 2000 (hereinafter the **FTC Public Workshop**).[15] Finally, the Cellular Telecommunications & Internet Association[16] (hereinafter the **CTIA**), whose members include companies like AT&T Wireless,[17] Sprint[18] and Microsoft,[19] petitioned the FCC in November 2000 to begin a rule-making procedure for tracking the location of wireless-device users. It has asked the FCC to adopt rules that would prohibit the collection of location data from wireless phone users unless they have opted in to such collection (hereinafter the **CTIA Petition**).

This paper is, therefore, meant to propose a solution, demonstrating how a LBS Provider may translate the privacy legal framework into business practices. More specifically, such translation includes the adoption of the appropriate business model and the development of adequate technological platforms and standards in order to provide consumers with personalized *push* location-based services.

First an introduction to location-based services, wireless personalization and location determination tracking technologies will be made. Such introduction will be followed by an analysis of the legal framework related to the privacy issues addressing the disclosure, choice and consent, quality, and security of the collected data, the transfer of such data and access to the data collected. Also, an analysis of the specific issues related to this new type of location-specific services through each of the subsections previously mentioned and analyzed under the legal framework will be made. Finally, a proposed business model and technology will be detailed, suggesting how LBS Providers may provide this new type of service, while preserving the privacy of wireless users and while also complying with the relevant North American and European privacy legal framework.

---

15 Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging technologies and Consumer Issues*, December 11-12, 2000. http://www.ftc.gov/opa/2000/11/wireless.htm (Last accessed on July 8, 2002)

16 A trade group representing cellular, PCS and enhanced specialized mobile radio carriers. http://www.ctia.org/ (Last accessed on July 8, 2002)

17 AT&T Wireless is a provider of advanced wireless voice and data services for consumers and businesses in North America. http://www.attws.com/ (Last accessed on July 8, 2002)

18 Sprint is a communications company, offering a diverse portfolio of products and services including long distance, local service, wireless, high-speed Internet, data services and more. http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

19 http://www.microsoft.com/ (Last accessed on July 8, 2002)

1 Location Data and Personalized Location-based Services

Personalized location-based services allow wireless users to receive relevant services relative to their geographic location. This location-specific type of personalization is also attractive to consumers, as they are able to receive targeted and relevant information at the right time and place.

Location-specific services and personalization in the wireless world are achieved through the use of location data gathered by location determination tracking technologies. More specifically, personalization is achieved through the use of historical location data and real-time location data, as further defined and detailed under Subsections 1.3.2 and 1.3.3.

1.1 Location-based Services

According to Ovum's research,[20] the market for location-based services is expected to top $20 billion by 2006.[21] With the advent of location technology, location-based services have begun proliferating in the wireless market on a global scale and Ovum believes it will soon have a wide presence in the world.

The following services are examples of location-specific types of services that could be offered to wireless users:

- **Safety and Emergency Services:** Personal Emergency Services would allow wireless users to contact private emergency response centers, and also allow emergency roadside assistance to locate and provide assistance to drivers in emergencies.[22] Imposed by the FCC in a recent ruling, E911 will be available to all wireless users in the United States. More specifically, E911 will enable all emergency response services, such as police, fire stations, and ambulances, to locate a caller specifically by tracking down the position of his wireless device. E911 will be mandatory for all U.S. carriers to deploy and be able to locate a caller in distress within a 125-meter range.

---

20 Ovum is an analyst and consulting company active in the Telecoms, IT, e-commerce, and digital media sectors. http://www.ovum.com/ (Last accessed on July 8, 2002)

21 Rosalie Nelson, *Mobile Advertising: building alternative revenue streams*, OVUM, Short Report 20, June 2000.

22 Strategis Group, *Wireless Location Services: 1999*, October 20, 1999.

Currently, there are several companies working to provide this service on a wide scale, such as Cell-Loc,[23] Qualcomm's[24] SnapTrack, and SignalSoft.[25] Companies such as the American Automobile Association[26] (hereinafter the **AAA**) and the Canadian Automobile Association[27] (hereinafter the **CAA**) are looking to provide services similar to E911, but only in order to provide their own services, such as towing, simple automotive repairs, and others. For example, consumers for safety measures may request emergency roadside assistance and airbag deployment notification services. The GM Onstar[28] vehicle navigation system using the GPS tracking technology can be used for its mapping capabilities, for safety in emergency situations, and for security in case of auto theft.

- **Traffic, Navigation Information and Roadside Assistance:** Services such as location-specific traffic updates and information and *intelligent* navigation instructions and services could be provided to wireless users.[29] Such services would enable these users to access precise directions to the destination of their choice using their location at the time of call as a starting point. Navigation instructions could be provided by a number of centered calling stations, dispersed throughout the given geographical area. Also, traffic information could be provided to wireless users, offering the latest updates and traffic conditions in their immediate area or along their regular route.

- **Directory, News, and Information Services:** Information services are currently being used by several click-and-mortar companies,[30] as part of a larger marketing focus whereby proximity and immediacy is key. Courier companies, clothing retailers, restaurant chains and bookstores have all

---

23 Cell-Loc Inc. is a marketer of a patented technology, known as the Cellocate System, which is capable of locating any wireless phone through existing networks. http://www.cell-loc.com/ (Last accessed on July 8, 2002)

24 QUALCOMM is best known as the company that pioneered Code Division Multiple Access (CDMA) technology, which is now used in wireless networks and handsets all over the world. http://www.qualcomm.com/ (Last accessed on July 8, 2002)

25 SignalSoft Corporation's Wireless Location Services® software suite allows carriers to provide location-based services to their subscribers. http://www.signalsoftcorp.com/ (Last accessed on July 8, 2002)

26 American Automobile Association (or the AAA) is one of the largest motoring services organization and leading provider of roadside assistance throughout the U.S. and Canada. The AAA is a not-for-profit, publicly-supported charitable educational and research organization dedicated to saving lives and reducing injuries by preventing traffic crashes. http://www.aaafoundation.org/home/ (Last accessed on July 8, 2002)

27 The Canadian Automobile Association is an advocate for Canada's motoring and travelling public. http://www.caa.ca/ (Last accessed on July 8, 2002)

28 http://www.onstar.com/ (Last accessed on July 8, 2002)

29 Strategis Group, *Wireless Location Services: 1999*, October 20, 1999.

30 Click-and-mortar describes a store that exists online and in the physical world.

recently incorporated reaching consumers on their wireless devices as part of their marketing strategies. Wireless users will be able to locate what they need by contacting an operator, which would provide the phone number, address, and directions to the desired destination. Users will be able to locate the nearest gas station, ATM machine, or other commonplace businesses through one unique number. Enhanced 411 would provide location-specific information and directory assistance services[31] and information to wireless users such as local weather reports, news, hotel and restaurant information, traditional news, and time/location-sensitive news, such as traffic information. Index Only Technologies,[32] Via-vis Mobile Solutions,[33] and ClickADeal.com[34] are introducing location-based business directory information with specialized services such as nearby gas stations, restaurants, and other stores along with their price comparisons and coupons.

- **Network Services and Location-based Billing:** Location-based billing is based on the idea that a variable rate and calling plan would give carriers the means to improve their present billing structures and be available based upon the location of the caller.[35] As a matter of fact, discounts applied to calls made from certain locations, to position wireless as an alternative to landline services, could be offered to wireless users.[36] For example, users could use their wireless phones for free at home, or at the office, and be billed on a pay per minute basis for other locations between home and the office. Higher pay-per-minute rates could be charged for calls made outside these locations and for long distance calls made.

- **Travel, Finance Services and Alerts:** Wireless users may want to be able to access their balance checking or be able to purchase, sell and get stock quotes depending on their location.[37] These users could subscribe to flight information, rental, car booking and travel report services, based on their location.[38] Wireless users are presently able to retrieve financial information, such as real-time stock quotes, stock price alerts, and related news updates from their wireless devices.

---

31 Strategis Group, *Wireless Location Services: 1999*, October 20, 1999.

32 http://www.indexonly.com (Last accessed on July 8, 2002)

33 http://www.viavis.com (Last accessed on July 8, 2002)

34 http://clickadeal.com/ (Last accessed on July 8, 2002)

35 Strategis Group, *Wireless Location Services: 1999*, October 20, 1999.

36 *Id.*

37 Adam Daum, *The Mobile Consumer*, GARTNER INC., Symposium ITxpo 2000, Orlando, Florida, October 2000, p. 4.

38 *Id.*

Content providers providing for such services include the Fidelity Group,[39] which offers the service through Sprint PCS wireless web,[40] and through Verizon wireless web.[41]

- **Entertainment:** Wireless users may be interested in receiving a service that would provide them with movie schedules, locations and reviews based on their location, for example when and if they are downtown on a weekend night. Others may be interested in a dating service that would alert them if someone corresponding to the desired profile were in their area. At the same time, a content provider, like a specific coffee shop, may want to sponsor this dating service by inviting these people, through their wireless devices, to meet at the closest coffee shop for a free coffee. Other sponsored services like Buddy Lists and Interactive Gaming could also be available to wireless users. Companies such as Invertix[42] and iProx[43] have developed Instant Messaging software products for wireless phones that alert other users on an individual's buddy list when they are in close proximity. NTT DoCoMo[44] has a similar *Friends Finder* service in Japan that provides the location of the user to his friends.[45] The wireless user has defined the persons who are allowed to see his location beforehand. The service is based on pushing the location data when a friend is, for example, within half a kilometer range.

- **M-commerce and Shopping Support:** Wireless users who are shopping may appreciate a sponsored service that would enable them to do an immediate comparison between CD and book prices online and in the shop.[46] Possibilities include shoppers comparing prices and product features at the point of sale.[47] Technologies such as precise location sensing may enable new types of applications, such as shopping support portals, which find alternative sources for products and services near the customer's location. Business needs new types of mobile applications to reduce

---

39 Fidelity Investments is an international provider of financial services and investment resources that help individuals and institutions meet their financial objectives. http://www100.fidelity.com/ (Last accessed on July 8, 2002)

40 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

41 Verizon Wireless is a wireless communications provider in the U.S., with the largest wireless network and more than 29.4 million customers. http://www.verizonwireless.com/mobileweb/ (Last accessed on July 8, 2002)

42 http://www.invertix.com/ (Last accessed on July 8, 2002)

43 http://www.iprox.com (Last accessed on July 15, 2001)

44 NTT DoCoMo is a provider of mobile communications in Japan. http://www.nttdocomo.com/top.html (Last accessed on July 29, 2001)

45 Sami Levijoki, *Privacy vs Location Awareness*, Helsinki University of Technology, Department of Computer Science, 2000. http://www.hut.fi/~slevijok/privacy_vs_locationawareness.htm (Last accessed on July 8, 2002)

46 Adam Daum, *The Mobile Consumer*, GARTNER INC., Symposium ITxpo 2000, Orlando, Florida, October 2000, p. 4.

47 Nick Jones, *Mobile Commerce Business Scenario*, GARTNER INC., Symposium ITxpo 2001, Orlando, Florida, October 2001.

costs, satisfy the need for *anywhere/anytime* customer service, and bridge supply chain gaps.[48] For example, GeePS[49] markets its wireless promotional systems to work within a shopping center.

- **Location-based Advertising:** This type of service consists of the delivery of advertisements, coupons and other forms of promotional and transaction-driven content to wireless devices based on their geographical position.[50] These messages may be delivered in multiple formats: alerts/messages pushed to the wireless users on their WAP phones, PDAs, two-way pagers and SMS-enabled devices.

Wireless marketing has been defined as the "total activities involved in communicating to a mobile audience through the use of un-tethered devices with the goal of increasing awareness, disseminating information, and promoting the sale of goods or services."[51] Using the medium for sales and promotion alerts that give consumers an instant benefit will also be very effective, and is one of the few ways to reach consumers directly with a timely incentive at the point of interest.

Windwire[52] executed a national U.S. trial of wireless advertising where millions of wireless ads were delivered to wireless users who access their favorite web content using phones, two-way pagers, and PDAs in the fall of 2000. It published its report in December of the same year that stated that sixty-four percent (64%) of the participants were concerned with privacy issues and to *push* wireless advertising in particular.[53]

Authors are unanimous in saying that there are many privacy issues surrounding wireless advertising. For example, Khan Basheera in an article entitled: *Mobile Marketing Takes SMS into the Future* was stating the following:

---

48 Bob Egan, *Mobile and Wireless Computing: The Next User Revolution*, GARTNER INC., Symposium ITxpo 2001, Orlando, Florida, October 2001.

49 http://www.geeps.com/ (Last accessed on July 15, 2001)

50 Gary W. Ozanich, *The Wireless Marketing Opportunity*, THE KELSEY GROUP, April 10, 2001, p. 1.

51 Windwire Inc., *First-to-Wireless: Capabilities and Benefits of Wireless Marketing and Advertising Based on the First National Mobile Marketing Trial*, December 27, 2000, p. i.

52 Windwire's technology allows advertisers to easily deliver highly targeted offers that are ideally formatted for each consumer's unique wireless device. http://www.windwire.com/ (Last accessed on July 8, 2002)

53 Windwire Inc., *First-to-Wireless: Capabilities and Benefits of Wireless Marketing and Advertising Based on the First National Mobile Marketing Trial*, December 27, 2000, p. 24.

> A critical aspect of successful mobile marketing lies in understanding the potential for intrusiveness of the medium – after all, most people carry their mobile phones round the clock – and respecting the need for the consumer's rights to decline receiving messages.[54]

There seem to be many businesses preparing to provide these new types of services. Already companies like Telcontar,[55] a developer of map engine software, market their product for potential commercial uses in advertising. Zebrapass[56] provided wireless ticketing and promotion solutions to sports, entertainment, and retail companies. Other companies like Profilium[57] and Avesair[58] are focusing on personalized location-based advertising.

Location-based, or wireless, advertising is the service that is the most likely to be intrusive since it may not be viewed as a *service* and it is most likely to be unsolicited. Also, wireless marketing needs to be as personalized and current as possible if wireless users are to let their device become a channel for companies to communicate with them. These users will expect companies to return the goodwill with valuable, personalized and relevant offerings. According to a study done by Quios[59] and Engage[60] on the efficacy of wireless advertising, personalization is especially important for wireless advertising.

According to the same study, wireless users are very accepting of advertising that is delivered within the context of relevant, value-added messages that match the user's profile.[61] Author Micah Kotch, in an article entitled: *Maximizing Mobile Marketing Opportunities*, was also confirming this opinion:

> Any meaningful long-term marketing relationship in the mobile space must take into account relevance to the end user. Permission-based marketing campaigns must allow for cultural and geographical nuances, including a traditional resistance to "push" services. In a global culture increasingly

---

54 Basheera Khan, *Mobile marketing takes SMS into the future*, IT WEB – the technology website, September 17, 2001. http://www.itweb.co.za/sections/quickprint/print.asp?StoryID=114578 (Last accessed on July 15, 2001)

55 http://www.telcontar.com/ (Last accessed on July 8, 2002)

56 http://www.zebrapass.com/ (Last accessed on July 15, 2001)

57 http://www.profilium.com (Last accessed on July 8, 2002)

58 http://www.avesair.com/ (Last accessed on July 8, 2002)

59 Quios is a global SMS distributor. http://www.quios.com/ (Last accessed on July 8, 2002)

60 Engage is a content management solutions provider. http://www.engage.com/ (Last accessed on July 8, 2002)

61 Quios and Engage, *The Efficacy of Wireless advertising*, Industry Overview and Case Study, 2000, p. 2.

> saturated by media of all kinds, the most powerful messages can be communicated through implicit trust and exchange of value. Carriers' core billing relationships with subscribers are an incredibly valuable asset that holds great potential for growing mutually profitable relationships well into the future. Trials across the world have shown subscribers will willingly opt-in for value-added services and are highly likely to respond to multiplayer competitions and branded promotions.[62]

Such personalization may be achieved through the recording and storage of the wireless user's historical geographic movement over time (or historical location data), that will be further analyzed and detailed under Subsection 1.3.2.

At the same time, many of the above-mentioned location-specific services may be sponsored by advertisers that would create campaigns, such as sponsored content alerts, providing consumers with value-added information, news, and updates, to reinforce their brand and encourage awareness or evaluation of a specific product. As a matter of fact, and as author Micah Kotch outlined in a Clickz report, advertisers will most likely play a significant sponsorship role in the financing of mobile data services:

> Wireless carriers in the United States need to take steps today to prepare for the proliferation of mobile advertising, because it will inevitably play a significant sponsorship role in the financing of mobile data services. Those carriers that best understand the potential - and potential pitfalls - of mobile as a marketing medium will be best positioned to take advantage of future revenues.[63]

For this reason and since advertisers are most likely to play an important role in the financing of these mobile services, location-based advertising should be considered as one of the most important location-based services.

1.2 Type of Location Tracking Technologies

In today's mobile communications networks, location data giving the geographic position of mobile users or, strictly speaking, that of their terminal equipment, already exist. Current wireless phone

---

62 Micah Kotch, *Maximizing Mobile Marketing Opportunities*, CLICKZ REPORT, October 5, 2001. http://www.clickz.com/wireless/ad_comm/article.php/897831 (Last accessed on July 8, 2002)

63 *Id.*

networks can locate a user based on the closest radio cell, to within a distance ranging from several meters to kilometers. This information is necessary to enable the transmission of communications from and to a user that does not have a constant fixed location. For cellular networks, the location data may be relatively imprecise, depending on the surface area of the cell within which the mobile user is at any given time.

Still, there are now not only one but two main kinds of tracking technologies available on the market in order to gather location data that carriers in the United States are deploying as we speak. These carriers are following the E911 mandate imposed by the FCC in a recent ruling, requesting all U.S. carriers to be able to locate a caller in distress within a certain distance for emergency purposes.[64] The main difference between these approaches is the place where the intelligence is derived, either in the device or within the network.

1.2.1 Network-based Location Method

The first solution includes network-based solutions that use cellular towers to describe the interconnection of signals with a user and which is the technology used by carriers like Verizon Wireless[65] and Western Wireless.[66]

For the purposes of routing incoming and outgoing calls, wireless networks inherently have the ability to track the location of wireless phones down to the nearest cell tower. As a matter of fact, networks can use the cell ID assigned to each active wireless phone to obtain very rough estimates of wireless users' locations.

According to Forrester Research,[67] these estimates are sometimes only accurate to within 30 kilometers.[68] Cell ID uses intelligence in the network to determine which cell is checking which base

---

64 http://www.fcc.gov/911/enhanced/ (Last accessed on July 8, 2002)

65 http://www.verizonwireless.com/ (Last accessed on July 8, 2002)

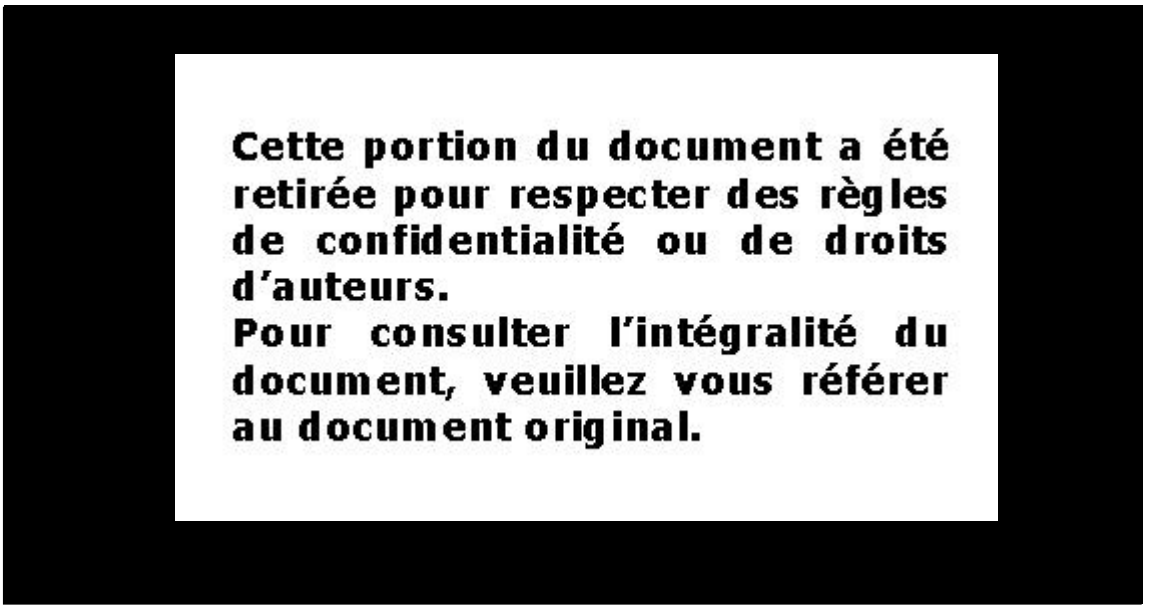
66 http://www.wwireless.com/ (Last accessed on July 8, 2002)

67 Forrester Research is an independent research firm that analyzes the future of technology change and its impact on businesses, consumers, and society. http://www.forrester.com/ (Last accessed on July 8, 2002)

68 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001.

station to offer the communicating phone the best reception.[69] To provide basic cell ID information, operators need a location server from an equipment manufacturer like Ericsson[70] that maps cells and base stations to X/Y coordinates.[71] Furthermore, such technology is the only type of technology that enables passive tracking of the wireless device as of today.

FIGURE No. 1 below illustrates and summarizes the network-based technology.



1.2.2 Handset-based Location Method

The second type of tracking technology is the handset-based solution which includes GPS and which is the technology used by other U.S. carriers including Sprint PCS,[72] Alltel[73] and Nextel[74] that favor handsets equipped with GPS receivers.[75]

---

69 *Id.* p. 3.

70 http://www.ericsson.com/ (Last accessed on July 8, 2002)

71 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, p. 3.

72 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

73 http://www.alltel.com/ (Last accessed on July 8, 2002)

74 Nextel Communications, based in Reston, VA, is a provider of fully integrated, wireless communications services on a large, all-digital, wireless network in the United States. http://www.nextel.com/ (Last accessed on July 8, 2002)

75 Simon Romero, *Location devices gain in popularity but raise privacy concerns*, N. Y. TIMES, March 4, 2001. http://www.nytimes.com/2001/03/04/technology/04LOCA.html (Last accessed on March 4, 2001)

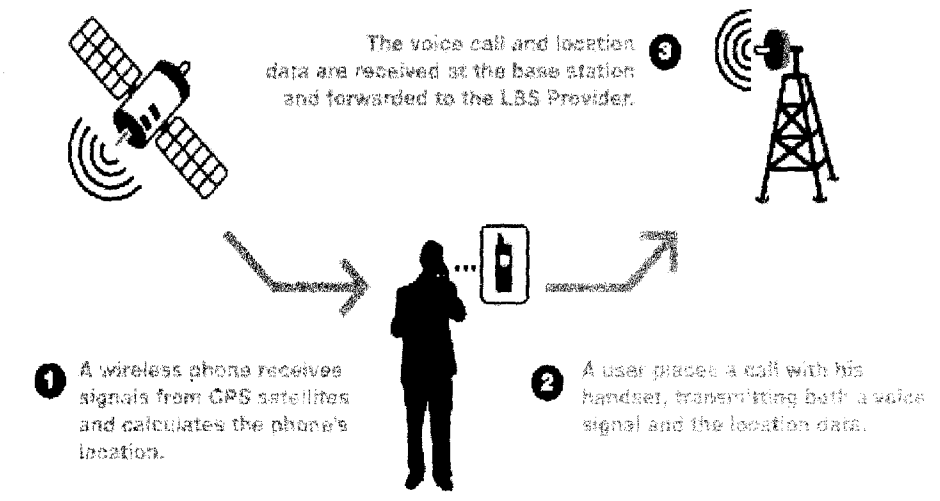
This type of location technology puts the onus of calculating the user's current position onto the individual handsets using GPS, which is the U.S. Department of Defense-funded satellite array now commercially available. Such technology uses an embedded chip in the handset to receive differential timing information from a satellite, which is in turn used to calculate the current location of the device.

The Global Positioning System requires GPS satellites orbiting earth to communicate with GPS chips in handsets. This type of technology is often used for emergency or health purposes. For example, Applied Digital Solutions has recently developed a wearable system called Digital Angel that features medical sensors, a GPS location chip and a wireless transmitter that can summon medical assistance for people who might otherwise be unable to obtain it.[76]

The GPS technology has accuracy precise within 1 meter.[77] On the other hand, GPS suffers accuracy problems in urban settings, even if carriers may enhance it with network technology, due to line-of-sight issues inherent in any satellite-driven technology. GPS is also not a reliable technology when the sky is not clear and if the GPS receiver is indoors.

FIGURE No. 2 below illustrates and summarizes the handset-based technology.

Handset-Based Technology



76 Bob Brewin, *Computerworld, Digital Angel to Watch Over Patients - But some fear system could be Big Brother,* January 1, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO55670,00.html (Last accessed on July 8, 2002)

1.2.3 Hybrid Method

By combining different kinds of location techniques, the availability and precision of the location data can be improved.

Carriers including VoiceStream[78] and AT&T Wireless[79] have requested deadline waivers from the FCC to develop and deploy hybrid E911 technology for handset-based and network-based systems in their various GSM[80] and TDMA[81] networks.[82] Such hybrid solutions may enable a carrier or a LBS Provider to benefit from the passive tracking function of the network-based method and the accuracy of the handset-based method at the same time.

1.3 Content Personalization and Location Data

According to the Personalization Consortium,[83] personalization is the use of technology and customer information to tailor interactions between a business and individual customers to fit a specific customer's stated or perceived needs. The goal is to make the interaction efficient and satisfying for both parties and to build a relationship that encourages loyalty. Forrester Research[84] is suggesting that in the same way as the ad networks such as DoubleClick[85] and Engage[86] are doing today, the best companies looking to send personalized content to wireless users (hereinafter **content providers**)

---

77 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, p. 4.

78 Based in Bellevue, WA, VoiceStream Wireless Corp. is a provider of digital wireless communications in the United States with 7 million subscribers. http://www.voicestream.com/ (Last accessed on July 8, 2002)

79 http://www.attws.com/ (Last accessed on July 8, 2002)

80 GSM means Global System for Mobile Communications, an open, non-proprietary system that provides international roaming capability. http://www.gsmworld.com/ (Last accessed on July 8, 2002)

81 Time division multiple access (TDMA) is digital transmission technology that allows a number of users to access a single radio-frequency (RF) channel without interference by allocating unique time slots to each user within each channel.

82 Jay Wrostad, *Where's the Fire? E911 Strategies Slow To Ignite*, WIRELESS NEWSFACTOR, June 7, 2001. http://www.wirelessnewsfactor.com/perl/story/10091.html (Last accessed on July 8, 2002)

83 The Personalization Consortium is an international advocacy group formed to promote the development and use of responsible one-to-one marketing technology and practices on the World Wide Web. http://www.personalization.org/ (Last accessed on July 8, 2002)

84 http://www.forrester.com/ (Last accessed on July 8, 2002)

85 DoubleClick is a provider of broad range of technology, media, direct marketing, email, and research solutions. http://www.doubleclick.com/ (Last accessed on July 8, 2002)

86 Engage is a content management solutions provider. http://www.engage.com/ (Last accessed on July 8, 2002)

based on such user's geographical location will understand the behavioral patterns of the wireless users. Using these patterns, content providers will be in a position to deliver context-relevant content,[87] which may make wireless users more accepting of location-based services or advertising according to a given study.[88]

The downside of personalization is, as outlined by the Center for Democracy and Technology[89] (hereinafter the **CDT**), the fact that profiling is threatening, and consumers have grown weary of practices such as the profiling of their preferences.[90] As a matter of fact, personalization on the Internet has been criticized and several lawmakers in the United States have moved to introduce legislation to regulate the use of personal information, data profile appending, and especially, the use of cookies to collect consumer data.[91]

In order to make the advertising message accurately personalized to each wireless user in a timely manner, many content providers may utilize a combination of three types of data that may be useful. The first type is personal, demographic or psychographic information about the user that may be used in the creation of the Static Profile of the wireless user as further explained under Subsection 1.3.1. The second type is the wireless user's historical location data that carriers or LBS Providers may gather and store over time in order to create Dynamic Profiles about these users' movement patterns, lifestyle, and habits though time as further explained under Subsection 1.3.2. Finally, the third type of data is real-time location data that may be useful to send a message to a wireless user that appears to be at the right location at the right time to make this message relevant as further explained under Subsection 1.3.3.

---

87 Goldman Sachs, *Technology: Mobile Internet*, MOBILE INTERNET PRIMER, United States, July 14, 2000, p. 5.

88 Quios and Engage, *The Efficacy of Wireless advertising*, Industry Overview and Case Study, 2000, p. 2.

89 The Center for Democracy and Technology is a non-profit organization that works to promote democratic values and constitutional liberties in the digital age and that has, since its inception in 1994, advocated for strong privacy rules that give individuals control over the collection, use and disclosure of personal information. http://www.cdt.org/ (Last accessed on July 8, 2002)

90 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CENTER FOR DEMOCRACY AND TECHNOLOGY, Comment (April 24, 2001), 22 pages, p. 8. (referring to the FTC's 2000 Online Profiling Report cited a Business Week/Harris Poll, indicated that "89% of consumers are not comfortable having their browsing habits and shopping patterns merged into a profile that is linked to their real name and identity," a common practice on the Internet. See OP Rept at 15.)

91 Kevin Mabley, *Privacy vs. Personalization – Personalization: A threat to privacy?*, CYBER DIALOGUE INC., 2000, p. 1.

On this issue, Steve Stutman, President and CEO of ClickaDeal.com[92] and participant at the FTC[93] Public Workshop, more specifically on the panel on location-based services and advertising entitled: *Possibilities and Privacy Concerns*, confirmed this distinction and the privacy issues surrounding the location data:

> Having said profile, another thing I would say is that there are static aspects of this which is to say user profile, user preferences, the sort of land marking that was discussed, which I would sort of roll into the profile, and then there's a dynamic content, and the dynamic content can be vendor pricing. It can be delays at O'Hare, can be a lot of different things, but as soon as you've said that, the question is how are you building a history. And if you have -- static information by definition is sort of a fixed history, if you will, but I think what we're really going to need to discuss as we do get into the privacy issues is how you keep track of the stuff that is dynamic.[94]

1.3.1 Static Profiling: Demographic and Psychographic Data

One way to make personalization work in the wireless world is to place consumers in charge of the process, as discussed by Evan Hendricks from Privacy Times.[95] Mr. Hendricks is of the opinion that the involvement of the wireless user will play a big role in the short term, and that a lot of the location-specific applications will be based on the profiles provided by the participants.[96]

For example, wireless users interested in receiving personalized location-based services may voluntarily provide information regarding their gender, age, interests, etc., to the LBS Provider in order to receive personalized content based on their Static Profile. Author Jon Silk, in his article *Brand New Message SMS Marketing Finds its Voice* was referring to a comment from AirMedia[97] to the effect that, in order to avoid spam and make their content relevant, companies wishing to provide

---

92 ClickaDeal is developing a suite of loyalty-based e-commerce applications. http://www.ClickaDeal.com/ (Last accessed on July 8, 2002)

93 http://www.ftc.gov/ (Last accessed on July 8, 2002)

94 Steve Stutman, President and CEO, ClickaDeal.com, participant at the Federal Trade Commission – Panel on location-based services and advertising: possibilities and privacy concerns, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 34. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

95 http://www.privacytimes.com/ (Last accessed on July 8, 2002)

96 Evan Hendricks, Privacy Times, participant at the Federal Trade Commission – Panel on location-based services and advertising: possibilities and privacy concerns, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 34. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

97 http://www.airmedia.com/ (Last accessed on July 15, 2001)

location-based advertising should ask personal information about the participant.[98]

1.3.2 Dynamic Profiling: Historical Location Data

The profiling of a wireless user may also be achieved through the collection and storage of such user's historical location data, or geographic movements over time (hereinafter **historical location data**), especially since a wireless device is time-sensitive and typically used by only one individual.[99] This allows service providers to push content based on this user's unique Dynamic Profile. The usage of location data to adapt the applications to the current location and provide the user information that is relevant to the current situation is based on the assumption that the relevance of the information is closely related to the location. For example, by analyzing all of the location data of a wireless user, it may be possible to extract a wealth of information about personal and commercial preferences, spending patterns, lifestyle, etc. that would provide a more accurate and updated profile of each individual.

This type of profiling is possible today mainly for service providers using network-based tracking technology, as opposed to handset-based tracking technology.[100] As a matter of fact, network-based technology tracks and stores the wireless user's location and movements in the carrier's network over time, monitoring the precise location of a wireless device whenever it is turned on, in passive mode.

This historical location data may be collected and archived, then used to build and create sophisticated wireless user profiles based on their movement patterns and habits through time and, based on this, provide them with personalized location-based content and services.

With location capability, it is also possible now to get a sense of where the user is at any point in time relative to where they may want to go, as was pointed out by Lorrie Faith Cranor from AT&T Labs Research:[101]

---

98 Jon Silk, *Brand new message SMS marketing finds its voice*, M-COMMERCE WORLD.COM, September 28, 2001. http://www.mcommerceworld.com/articles/article.cfm/952E7614-A21E-403B-A8AD8214DE36DE49 (Last accessed on September 28, 2001)

99 Mobilocity.net, *Seizing the M-Commerce Opportunity, Strategies for Success on the Mobile Internet*, White paper, May 2000.

100 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, p. 3.

101 http://www.research.att.com/ (Last accessed on July 8, 2002)

> For the most part service providers are not archiving this information. They just keep it until the next ten minutes when you check in and they find out you've moved to the next cell site. It's a huge amount of data, and for the most part they don't have anything that they're doing with it, but there are a lot of interesting business models that we've been hearing about that of course could make some really valuable use of that information. And it's really nice in these business models to know not only where you are now and where you were ten minutes ago but that for the past two weeks you've come here every day at this time, so keeping that kind of data is something I think we're going to see more and more of in the future.[102]

The problem is that over time, location data gathered by these LBS Providers and stored in databases could create a very detailed and invasive dossier of a person's movements. As a matter of fact, this technology would enable LBS Providers to deliver very helpful, location-specific information while also building detailed, *Big Brother-like* profiles of an individual's travel patterns and other habits.

1.3.3 Location-specific Profiling: Real-time Location Data

Finally, services must be tailored to the location and time schedules of customers. Customers' needs may vary depending on where they are and what time of day it is. For example, if it is Friday evening and a customer is in an unfamiliar city, the customer may be looking for restaurants or entertainment options within a geographic locale. In the morning, a customer may want to know the local weather forecast. At lunch he may want to check a stock quote.

Arthur D. Hurtado, CEO for Invertix[103] and participant on a Panel on generation and control of location data, was outlining the benefits of location data in order for wireless users to be provided with personalized content:

> Corresponding to the location data is the presence of information, that is, that you're on or off the net, that your buddy list is appearing as an instant message as an example, and third is the subscriber profile interest, the fact that one of us may want to have our interest known so that we can receive personalized, localized, customized kinds of information.[104]

---

102 Lorrie Faith Cranor, AT&T Labs research, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 5. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

103 Invertix is a supplier of instant messaging, presence, privacy and location solutions to mobile network operators. http://www.invertix.com/ (Last accessed on July 8, 2002)

104 Arthur D. Hurtado, CEO, Invertix, participant at the Federal Trade Commission – Panel on generation and control of location information,

Location data may provide the means to use real-time positioning as a trigger for marketing messages (hereinafter **real-time location data**). This is the only means for advertisers and content providers to reach wireless users in daily action, and send them sponsored marketing messages and services at the right time and place. This type of personalization is also attractive to consumers as it allows them to receive content and advertising messages relative to their geographic position and in a timely manner to make a message relevant.

Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues, Wireless Web Workshop, December 12, 2000, p. 29. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

2 European and North American Legal Framework

Many standards, laws or guidelines were recently drafted, and are being enacted as we speak, in order to solve privacy issues regarding the handling of individual's personal data. Most of the regulations already in place are related to personal information that would be collected, stored, and used by third parties. Before determining that these laws apply to location data, we have to ask ourselves the following question: *Does location data = personal data?*

An appropriate interpretation may be that location data is personal data if and only if it contains Personally Identifiable Information (hereinafter **PII**). PII has been defined as data which can be used to identify or contact a person uniquely and reliably, including but not limited to name, address, telephone number, e-mail address, and account or other personal identification number, as well as any accompanying data linked to the identity of that person.[105] Since these laws and regulations were put in place to protect personal information of the consumers, they may not apply when anonymous location data is stored and used by third parties since the purpose of protecting PII is no longer present.

Many laws or regulations are recently extending the notion of personal data to also include location data. For example, on 12 July 2000, the European Commission issued the 2000 EC Proposal for an amendment to the *EC Directive 97/66/EC*,[106] in order to update provisions to cope with technology evolution, such as the move from fixed to wireless communications and from voice to data. Such proposal was accepted in November 2001 by the European Parliament.[107] It introduces safeguards for wireless users with regards to location-based services,[108] and gives users the right to refuse unsolicited

---

105 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.waaglobal.org/ (Last accessed on July 8, 2002)

106 Article 9, Commission of the European Communities, *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* (presented to the Commission – Legislation under preparation), COM (2000) 385 Final, 2000/0189 (COD), Brussels (July 12, 2000).

107 European Union, *Proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector*, Bulletin EU 11-2001, Information Society 7/11, November 13, 2001. http://europa.eu.int/abc/doc/off/bull/en/200111/p103104.htm (Last accessed on July 8, 2002)

108 Article 9, Commission of the European Communities, *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* (presented to the Commission – Legislation

communications for direct marketing purposes, and it was extended to cover all forms of electronic communications.[109] The 2000 EC Proposal was eventually amended in January 2002[110] and these changes were translated into amendments to be incorporated in the *EC Directive 97/66/EC* in April 2002.[111]

U.S. bills introduced in 2001 like the *Wireless Privacy Protection Act*[112] and the *Location Privacy Protection Act*[113] seem to also associate location data to personal data.

Furthermore, the most important aspect about wireless technology is that each device, usually belonging to one specific individual, transmits a unique identifier, which enables the wireless phone to communicate and identify itself as it passes from one cell to another. Certain authors[114] are of the opinion that it is likely that enterprising companies will find ways to capture the unique identifier transmitted by wireless phones.[115] For this reason, these companies may be able to link the wireless phone's unique identifier with the true identity of the wireless phone user.

For all these reasons, the notion of *personal data* has been interpreted more broadly in the last few years and has included location data. This interpretation of personal data and inclusion of location data may be adequate, specifically given that location data is usually linked to a person uniquely, through the wireless phone number that usually belongs to that specific user. Furthermore, in many cases, either location data contains PII or at least there is a threat that location data be merged with PII or that personal information will be available through the storage of such data. Thus, an analysis of both regulations regarding the protection of personal data, as well as the attempts to regulate on the

---

under preparation), COM (2000) 385 Final, 2000/0189 (COD), Brussels (July 12 , 2000).

109 *Id.* Article 13.

110 Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

111 European Parliament, *II Recommendation for second reading on the Council common position for adopting a European Parliament and Council directive concerning the processing of personaln data and the protection of privacy in the electronic communications sector*, Committee on Citizen's Freedoms and Rights, Justice and Home Affairs, Final (April 22, 2002).

112 The Wireless Privacy Protection Act , HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

113 The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

114 including Evan Hendricks from the Privacy Times. http://www.privacytimes.com/ (Last accessed on July 8, 2002)

115 Evan Hendricks, *Wireless location Technology: The Ultimate Challenge to Privacy*, Before the XXIII International Conference Of Data

protection of location data, will be done in the present paper.

2.1 Disclosure

More specifically with regards to the disclosure issue, laws and regulations regarding the protection of personal data seem to be unanimous to the effect that the collector of such data should disclose the purpose of the collection to the subject.

The *OECD Guidelines*[116] are explicit to the effect that the purposes for which personal data are collected should be specified not later than at the time of data collection.[117] These guidelines also state that there should be a general policy of openness about developments, practices and policies with respect to personal data.[118] Also, means should be readily available to establish the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller.[119]

In Europe, *Directive 95/46/EC*[120] states that personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[121] It also states that the data collector must provide the subject from whom data is collected the purposes of the processing for which the data are intended.[122] According to the 2000 EC Proposal, service providers must, prior to obtaining consent for such services, inform the user of the types of data which are processed.[123] They must also inform such users of the duration of such processing for the purposes related to subscriber billing and interconnection payments, for the

---

Protection Commissioners, September 24, 2001.

116 OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980).

117 *Id.* Article 9.

118 *Id.* Article 12.

119 *Id.*

120 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

121 *Id.* Article 6 a).

122 *Id.* Article 10 b).

123 Article 6 (4), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

purposes of marketing electronic communications services or the provision of value-added services.[124] Such service providers must also inform the users, prior to obtaining their consent, of the type of location data[125] other than traffic data[126] which will be processed and the purposes and duration of the processing.[127] Furthermore, the data collector shall inform the user on whether the data will be transmitted to a third party for the purpose of providing value-added services.[128]

In the United States, the *Safe Harbor Agreement*[129] went into effect on November 1, 2000. Such Agreement is designed to provide some legal protection to U.S. companies and organizations that, as part of their European operations, gather PII about people living there, and to adequately meet the European Union's data Privacy Directives, which are more stringent than current U.S. privacy law. The *Safe Harbor Agreement* states that an organization must inform individuals about what type of personal information it collects, how it collects that information and the purposes for which it collects such information.[130] An organization must also inform the users about the types of organizations to which it discloses the information and the choices and means the organization offers individuals for limiting its use and disclosure.[131] It also specifies that this notice must be provided in clear and conspicuous language that is readily understood and made available when individuals are first asked to provide personal information to the organization.[132]

Also in the United States, many bills were introduced in the last year in order to promote the protection of the wireless user's location data. Even if some of these bills are not enacted, they do reflect a certain trend on how things should be done in the wireless world since they are to the point and are a product of a collective reasoning on certain wireless privacy issues.

---

124 *Id.*

125 Location data shall mean, in accordance with the 2000 EC Proposal, an electronic communications network, indicating the goegraphic position of the terminal equipment of a user of a publicly available electronic communications service.

126 Traffic data shall mean, in accordance with the 2000 EC Proposal, any data processed in the course of or for the purpose of the transmission of a communication over an electronic communications network.

127 Article 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

128 *Id.*

129 U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

130 *Id.* Article 1.

131 *Id.*

The *Wireless Privacy Protection Act*[133] was introduced by Mr. Frelinghuysen in the House of Representatives on January 30, 2001. This bill requires that the wireless users must be given the opportunity to choose whether, and the manner in which, a third party uses the personal information they provide, when such use is unrelated to the use(s) for which they originally disclosed it.[134] Also, and with regards to the disclosure, a customer shall not be considered to have granted express prior authorization unless the carrier has provided the customer in writing a clear, conspicuous, and complete disclosure of the carrier's practices with respect to the collection and use of location data.[135] This shall be done before any such information is disclosed or used.[136] Furthermore, such disclosure should include a description of the specific types of information that is collected by the carrier[137] and details on how the carrier uses such information.[138]

Also, the *Location Privacy Protection Act*[139] was introduced in the U.S. Senate in July 2001 in order to protect the privacy of users of wireless devices that pinpoint their location. This bill was introduced by Senator John Edwards who had previously introduced the Spyware Control and Privacy Protection Act in January 2001 to protect the privacy of people who use computer software programs that secretly track their shopping habits and other interests.[140] The bill states that LBS Providers have to inform customers (or wireless users), with clear and conspicuous notice, about their policies on the collection, use, disclosure of, retention of, and access to their location data.[141]

---

132 *Id.*

133 The Wireless Privacy Protection Act , HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

134 Article 3, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

135 Article (1) (A), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

136 *Id.*

137 *Id.*

138 *Id.* Article (1) (B).

139 The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

140 United States Senate, *Senator Edwards proposes location privacy law*, North Carolina, Press Release, July 11, 2002. http://edwards.senate.gov/press/2001/jul11-pr.html (Last accessed on July 8, 2002)

141 Section 3, Article (b) (1) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

In Canada, the *Personal Information Protection and Electronic Documents Act*[142] (hereinafter **PIPEDA**) has recently become law, requiring businesses to offer Canadian citizens certain guarantees regarding the collection and use of personal data. The Act is based on the *CSA Model Code for the Protection of Personal Information*,[143] which is a standard that has the potential to operate in the same way as many other quality-assurance standards such as the increasingly popular ISO 9000 series. The CSA Model was put in place in 1995, motivated by the European Union *Directive 95/46/EC* and by the fear that "European Commission member countries may be reluctant to share personal data with Canadian businesses, potentially creating a trading block of immense consequence."[144]

The Honorable Brian Tobin, Minister of Industry, and the Honorable Pierre Pettigrew, Minister of International Trade, announced in January 2002 that the European Commission had ruled that PIPEDA met the rigorous European Union standards for the protection of personal data.[145] This unanimous decision by the European Parliament and Commission allowed for the continued flow of personal information between the European Union and Canada.

PIPEDA, which initially applies only to federally regulated companies as of January 2001, will extend by 2004 to every organization that collects, uses or discloses personal information in the course of a commercial activity, whether or not the organization is a federally-regulated business. This means that an organization may only collect, use or disclose personal information for purposes that a reasonable person would consider are appropriate in the circumstances[146] and with the knowledge or consent of the individual.[147] The law states that the identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.[148] Depending upon the way in which the information is collected, this can be done orally or in writing.[149] An application form, for example, may give notice of the purposes.[150]

---

142 Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

143 Canadian Standards Association, CSA Standard CAN/CSA-Q30-96, *Model Code for the Protection of Personal Information*, A National Standard (March 1996).

144 Canadian Standard Association, *Privacy Code a must for global economy*, Focus, Spring 1992.

145 Industry Canada, *European Commission Recognizes Canadian Legislated Privacy Protection*, Ottawa, January 14, 2002.

146 Article 5 (3), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

147 *Id.* Article 7.

148 *Id.* Schedule 1, Section 5, Article 4.2.3.

149 *Id.*

150 *Id.*

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified and the consent of the individual is required before information can be used for that purpose.[151] Also, an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.[152] The information made available shall include the name, or title, and the address of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded.[153] Such information shall also include the means of gaining access to personal information held by the organization,[154] a description of the type of personal information held by the organization,[155] information that explain the organization's policies, standards, or codes,[156] and what personal information is made available to related organizations like subsidiaries.[157] An organization may make information on its policies and practices available in a variety of ways and the method chosen depends on the nature of its business and other considerations.[158]

Finally, an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice,[159] and the organization shall inform the individual of the implications of such withdrawal.[160]

Quebec was the first legislature in North America to pass an *Act Respecting The Protection of Personal Information In The Private Sector.*[161] In accordance with such Act, a person who collects personal information from a person concerned must, when establishing a file on that person, inform

---

151 *Id.* Schedule 1, Section 5, Article 4.2.4.

152 *Id.* Schedule 1, Section 5, Article 4.8.

153 *Id.* Schedule 1, Section 5, Article 4.8.2 (a).

154 *Id.* Schedule 1, Section 5, Article 4.8.2 (b).

155 *Id.* Schedule 1, Section 5, Article 4.8.2 (c).

156 *Id.* Schedule 1, Section 5, Article 4.8.2 (d).

157 *Id.* Schedule 1, Section 5, Article 4.8.2 (e).

158 *Id.* Schedule 1, Section 5, Article 4.8.3.

159 *Id.* Schedule 1, Section 5, Article 4.3.8.

160 *Id.*

161 Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada). Such Act has the object of establishing, for the exercise of the rights conferred by articles 35 to 40 of the *Civil Code of Quebec* concerning the protection of personal information, particular rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to

him of the object of the file.[162] Such collector must also inform the person concerned of the use which will be made of the collected information and the categories of persons who will have access to it within the enterprise.[163] It shall also inform the subject where the file will be kept and the rights of access.[164] The recent *Act to Establish a Legal Framework for Information Technology*[165] states that a person may not be required to submit, for identification purposes, to a process or device that affects the person's physical integrity.[166] In accordance with the same law, unless otherwise expressly provided by law for health protection or public security reasons, a person may not be required to be connected to a device that allows the person's whereabouts to be known.[167]

On the industry side, many players have been active in either proposing privacy guidelines for these types of services or in ensuring that others are changing the rules in order to protect the privacy of wireless users. As previously mentioned, the FTC at its December 2000 Public Workshop was already exploring wireless privacy issues.[168]

CTIA submitted a proposal in 2000 for privacy guidelines for location-based services to the FCC[169] and also initiated procedures to force such Commission to initiate a separate rulemaking proceeding, distinct from the Commission's Customer Proprietary Network Information (hereinafter **CPNI**)[170] docket, to address the location privacy issues raised by CTIA's Petition. CTIA states that LBS Providers must inform the customer (or wireless user) about the specific location data collection and use practices before any disclosure or use of location data takes place.[171]

---

third persons in the course of carrying on an enterprise within the meaning of article 1525 of the *Civil Code of Quebec*.

162 Article 8, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

163 *Id.*

164 *Id.*

165 Act to Establish a Legal Framework for Information Technology, Bill 161, 36th legislature, 2nd session, c. 32 (2001) (Quebec, Canada).

166 *Id.* Article 43.

167 *Id.*

168 Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging technologies and Consumer Issues*, December 11-12, 2000. http://www.ftc.gov/opa/2000/11/wireless.htm (Last accessed on July 8, 2002)

169 Simon Romero, *Location devices gain in popularity but raise privacy concerns*, N.Y.TIMES, March 4, 2001. http://www.nytimes.com/2001/03/04/technology/04LOCA.html (Last accessed on March 4, 2001)

170 CPNI is defined as carrier's data about a specific customer's service and usage.

171 By "collection", CTIA means the acquisition of location data other than that used to complete a call or provide a subscriber access to a network. In most wireless systems, a user's rough location (i.e., the nearest cell site) is known to the network and is an integral part of completing wireless calls. This is not considered "collection" activity according to CTIA: See Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy

The Wireless Advertising Association,[172] now working under the name of Mobile Marketing Association (hereinafter **MMA**) since January of 2002,[173] is a group of carriers, advertising agencies, device manufacturers, and wireless advertising providers involved in establishing guidelines for any wireless advertising medium. The MMA has established guidelines with regards to privacy policies for wireless advertising companies that were intended to complement and supplement the notice and choice provisions of the *Self-Regulatory Principles for Online Marketing for Network Advertisers* endorsed by the FTC and the U.S. Department of Commerce on July 27, 2000.[174] MMA is of the opinion that its members' disclosure should take the form of a privacy policy. Such policy should state the type of information being collected, their policy on data storage, the possible third party distribution of that information, their commitment to data security and information related to the quality of the collected data.[175]

Finally, the Wireless Location Industry Association (hereinafter **WLIA**) is the voice of the emerging wireless location industry.[176] Its member companies provide hardware, software, services and other products related to the new ability to locate the precise origin of wireless radio signals that add consumer value based on the geographic locations of wireless device users. In November 2001, it established privacy policy standards and guidelines for member companies setting acceptable standards for protection of the individual privacy of users of wireless devices that may be located using signal location technology.[177]

Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 9.

172 WAA was initially formed by the merger of the Wireless Advertising Industry Association and the Internet Advertising Bureau's Wireless Ad Council. http://www.mmaglobal.com (Last accessed on July 8, 2002)

173 Mobile Marketing Association, *WAA And WMA Merge To Expand Global Forum For Standards In Mobile Marketing - Leading industry bodies join forces to set standards and deliver new benefits for members*, Press Release, January 10, 2002. http://www.waaglobal.org/press/merger1-10_press.shtml (Last accessed on July 8, 2002)

174 http://www.networkadvertising.org/aboutnai_principles.asp (Last accessed on July 22, 2002)

175 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002)

176 http://www.wliaonline.org/ (Last accessed on July 8, 2002)

177 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

More specifically with regards to disclosure issues, the WLIA states that privacy policies should be clear and conspicuous, and should be easy to find, read and understand.[178] No prospective wireless user should reach the point of subscription to a location-based service without being confronted with an invitation to review the privacy policy of the LBS Provider.[179] Also, the policy must be available to the wireless user prior to or at the time that geographically tagged PII is collected or requested.[180] The policy may be accessible on or included with the service contract, on wireless devices, when technically feasible, or available elsewhere, generally including but not limited to websites, so long as it is readily accessible to wireless users and the public.[181] WLIA members should notify wireless users of any substantive changes to their privacy policies and the reason for the change.[182] They should also take steps to ensure that these standards are adopted and/or made a condition of doing business with business partners, technology providers and other partners.[183]

According to the WLIA privacy guidelines, the policy or disclosure must include the following information: (i) the nature of the information being used and/or collected, (ii) the WLIA member's policy on data ownership and storage, including whether any geographically tagged PII is used or collected,[184] (iii) the use of that information, including possible or actual third-party distribution of that information, (iv) a statement of the organization's commitment to data security, (v) the specific steps that the organization takes to ensure data quality and access by the user to their own geographically tagged PII, (vi) the process by which a wireless user can propose to correct any wrong information, and (vii) contact information within the company for questions or additional information about data collection, use and disclosure within the company.[185]

Please refer to Schedule "A" in order to view the Summarizing Chart on the legal framework relating to the disclosure privacy issues.

---

178 *Id.*

179 *Id.*

180 *Id.*

181 *Id.*

182 *Id.*

183 *Id.*

184 e.g. whether particular information is mandatory or optional.

185 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

2.2 Choice & Consent

The legal framework regarding the consent issue is related to the protection of the wireless user's personal data and to the protection against wireless spam.

2.2.1 Regulations Related to the Collection or Use of Personal and Location Data

According to the *OECD Guidelines*,[186] where appropriate, the collection of personal data and any other data should be obtained with the knowledge or consent of the data subject.[187] Furthermore, such collection should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Article 9 of the Guidelines, except with the consent of the data subject.[188] In Europe, the *EC Directives*[189] state that personal data may be processed only if the data subject has unambiguously given his consent.[190] The data subject also has to have the right to object, on request and free of charge, to the processing of personal data relating to him, which the controller anticipates being processed for the purposes of direct marketing.[191] According to the 2000 EC Proposal, the provider of a publicly available electronic communications service may also process the data for the purpose of marketing electronic communications services or for the provision of value-added services.[192] This may only be done for the duration necessary for such services or marketing, if the wireless user to whom the data relate has given his consent[193] and if it has been given the possibility to withdraw his consent for the processing of the location data at any time.[194]

---

186 OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980).

187 *Id.*Article 7.

188 *Id.* Article 10 a).

189 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995) and Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

190 Article 7 a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

191 *Id.* Article 14 b); and Articles 11 1) and 12 1), Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

192 Article 6 (3), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

193 *Id.*

194 *Id.* Article 9 (1).

More specifically, where consent of the users has been obtained for the processing of location data, the user must continue to have the possibility of temporarily refusing the processing of such data for each connection to the network.[195] This shall be done using a simple means and shall be free of charge.[196] Finally, when location data can be processed, such data may only be processed when they are made anonymous, or with the consent of the users.[197]

In the United States, the *Safe Harbor Agreement*[198] states that an organization must give individuals the opportunity to choose whether and how the personal information they provide is used and where such use is unrelated to the use(s) for which they originally disclosed it.[199] It further mentions that this should be done through an opt-out procedure.[200]

The *Wireless Privacy Protection Act*[201] is a bill recently introduced in the United States. Such bill requires that a customer shall not be considered to have granted express prior authorization unless the carrier has provided to the customer in writing a clear, conspicuous, and complete disclosure of its practices with respect to the collection and use of location data.[202] Furthermore, this shall be done before any such information is disclosed or used unless the customer has agreed in writing to such collection and use.[203] Another bill introduced in the United States in July of 2001, the *Location Privacy Protection Act*,[204] requires LBS Providers to obtain a customer's express authorization before collecting, using, or retaining the customer's location information.[205] Also, LBS Providers shall obtain the customer's consent prior to disclosing or permitting access to the customer's location data to any person who is not a party to, or who is not necessary to the performance of, the service contract

---

195 *Id.* Article 9 (2).

196 *Id.*

197 *Id.* Article 9 (1).

198 U.S. Department of Commerce, *Safe Harbor* Agreement (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

199 *Id.* Article 2.

200 *Id.*

201 The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

202 *Id.* Article (2).

203 *Id.*

204 The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

205 *Id.* Section 3, Article (b) (1) (B) (i).

between the customer and such provider.[206] The methods, whether technological or otherwise, by which a customer may provide express prior authorization may include a written or electronically signed service agreement or other contractual instrument.[207]

In Canada, PIPEDA[208] mentions that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances[209] and with the knowledge or consent of the individual.[210] Such law states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.[211] To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.[212] The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information.[213] In determining the form of consent to use, organizations shall take into account the sensitivity of the information.[214] Furthermore, the way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected.[215] Finally, an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice[216] and the organization shall inform the individual of the implications of such withdrawal.[217] Even if PIPEDA is not clear on the way to gather a wireless user's consent, a recent release from the Privacy Commissioner of Canada states that opt-in is a much better way to do so.[218]

---

206 *Id.* Section 3, Article (b) (1) (B) (ii).

207 *Id.* Section 3, Article (b) (4) (A).

208 Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

209 *Id.* Article 5 (3).

210 *Id.* Article 7.

211 *Id.* Schedule 1, Section 5, Article 4.3.

212 *Id.* Schedule 1, Section 5, Article 4.3.2.

213 *Id.* Schedule 1, Section 5, Article 4.3.4.

214 *Id.*

215 *Id.* Schedule 1, Section 5, Article 4.3.6.

216 *Id.* Schedule 1, Section 5, Article 4.3.8.

217 *Id.*

218 Privacy Commissionner of Canada, *Findings regarding complaints about Air Canada's Aeroplan Frequent Flyer Program under the Personal Information Protection and Electronic Documents Act*, New release, Ottawa, March 20, 2002. http://www.privcom.gc.ca/media/nr-c/02_05_b_020320_e.asp (Last accessed July 8, 2002)

In Quebec, the *Act Respecting the Protection of Personal Information in the Private Sector*[219] states that the consent to the communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes.[220] Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.[221] As previously mentioned, the *Act to Establish a Legal Framework for Information Technology*[222] states that a person may not be required to submit, for identification purposes, to a process or device that affects the person's physical integrity.[223] Also, unless otherwise expressly provided by law for health protection or public security reasons, a person may not be required to be connected to a device that allows the person's whereabouts to be known.[224]

On the industry side, MMA members should give wireless users the opportunity to exercise choice regarding how their PII is used and the consent should be obtained through indigenous technological mechanisms available for wireless media.[225] The WLIA prescribes that its members shall give each authorized user for whom it may obtain geographically tagged PII the maximum reasonable opportunity to exercise choice regarding whether and when such user wishes to be located.[226] Such choice shall also cover how the user's geographically tagged PII is used and/or stored.[227] According to the WLIA Guidelines, each WLIA member must highlight portions of subscriber agreements indicating that the subscriber agrees to be located when he activates specific location-based features or services.[228] For such features or services, these subscribers will be considered to have given standard opt-in permission.[229] WLIA members should further notify, and seek standard opt-in consent from, subscribers of new services.[230] Finally, subscribers should be provided clear, easy to perform

---

219 Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

220 *Id.* Article 8.

221 *Id.*

222 Act to Establish a Legal Framework for Information Technology, Bill 161, 36th legislature, 2nd session, c. 32 (2001) (Quebec, Canada).

223 *Id.* Article 43.

224 *Id.*

225 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 4.

226 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

227 *Id.*

228 *Id.*

229 *Id.*

230 *Id.*

instructions on how to opt-out or disable location-based services.[231]

2.2.2 Regulations Related to Spam

In the context of the Internet, spamming or pushing unsolicited message has been an ongoing issue that has resulted in certain initiatives in Europe and the introduction of many anti-spam bills in the United States over the last few years.

In Europe, the proposed directive for an amendment to the *EC Directive 97/66/EC* issued by the European Commission[232] and accepted in November 2001 by the European Parliament[233] gives users the right to refuse unsolicited communications for direct marketing purposes and is extended to cover all forms of electronic communications.[234] More specifically, according to such 2000 EC Proposal, the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (faxes) or electronic mail for the purposes of direct marketing may only be allowed in respect to subscribers who have given their prior consent.[235] It is interesting to note that in the document emanating from the European Parliament dated April 2002, the proposed amendment also includes SMS, which is further define as the short message service available on wireless phones.[236] It further prescribes, in any event, that the practice of sending electronic mail for purposes of direct marketing shall be prohibited when the identify of the sender is disguised or concealed.[237]

---

231 *Id.*

232 Commission of the European Communities, *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* (presented to the Commission – Legislation under preparation), COM (2000) 385 Final, 2000/0189 (COD), Brussels (July 12, 2000).

233 European Union, *Proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector*, Bulletin EU 11-2001, Information Society 7/11, November 13, 2001. http://europa.eu.int/abc/doc/off/bull/en/200111/p103104.htm (Last accessed on July 8, 2002)

234 Article 13, Commission of the European Communities, *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* (presented to the Commission – Legislation under preparation), COM (2000) 385 Final, 2000/0189 (COD), Brussels (July 12, 2000).

235 Article 13 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

236 European Parliament, *II Recommendation for second reading on the Council common position for adopting a European Parliament and Council directive concerning the processing of personaln data and the protection of privacy in the electronic communications sector*, Committee on Citizen's Freedoms and Rights, Justice and Home Affairs, Final (April 22, 2002).

237 Article 13 (4), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a*

The practice of sending electronic mail without a valid address to which the recipient may send a request that such communications cease shall also be prohibited.[238]

The *Electronic Commerce Directive*[239] states that with regards to unsolicited commercial communications, member countries shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.[240]

The European Coalition Against Unsolicited Commercial Email[241] (hereinafter **CAUCE**) is a group of Internet users that have formed a coalition to promote legislation that would outlaw unsolicited commercial e-mail.[242] CAUCE is trying hard to promote the opt-in model as the scheme of choice and many European countries have enacted legislation promoting this last model for pushing advertising on the Internet side.[243]

The European Parliament voted on May 30, 2002, to accept a compromise on the proposed Directive for the protection of personal data and privacy in the e-communications sector.[244] The adoption of such Directive will result in having the European Union set an important worldwide precedent by adopting a harmonised opt-in approach to unsolicited commercial e-mail.[245] The opt-in will equally cover SMS messages and other electronic messages received on any wireless or fixed terminal.[246]

Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, 15396/2/01, Brussels (January 29, 2002).

238 *Id.*

239 Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1, European Union (2000).

240 *Id.* Article 7 (2).

241 EuroCAUCE http://www.euro.cauce.org/en/index.html

242 *Id.*

243 http://www.euro.cauce.org/en/countries/index.html (Last accessed on July 15, 2002) and http://www.euro.cauce.org/en/optinvsoptout.html (Last accessed on July 15, 2002)

244 European Commission, *Commission welcomes European Parliament's vote to accept directive on data protection rules for electronic communications sector*, Press release, IP/02/783, Brussels, May 30, 2002.
http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/02/783|0|RAPID&lg=EN (Last accessed July 8, 2002)

245 *Id.*

246 *Id.*

In the Unites States and also on the Internet side, many bills have been recently introduced to regulate spamming. In the last year, the bills introduced prohibit that these messages have false headers or deceptive subject lines;[247] they require that these messages be labeled[248] and that they include opt-out instructions.[249] On the wireless side, there is a recent bill introduced in January of 2001, the *Wireless Telephone Spam Protection Act*,[250] which accurately addresses wireless spam by prohibiting the use of wireless messaging systems to send unsolicited advertisements to wireless phones.[251]

Canada does not yet have a specific law regulating the use of unsolicited e-mail or wireless spam, though a July 1999 court case did find a website owner responsible for sending spam.[252] We can also refer to PIPEDA[253] that seems to imply an opt-in approach when it states that no information contained in a file can be used without the consent of the person concerned.[254]

On the industry side, the MMA is of the opinion that any push messaging should be sent to a wireless device only after a user's permission has been given through *confirmed opt-in*. Such *Confirmed opt-in* process is defined as a process of verifying a user's permission in order to ensure that push messaging and/or content is not accidentally or maliciously sent to the user's device. For example, after receiving permission from a user, an advertiser or marketer may send a message to the user to which he must positively reply in order to confirm permission to start receiving push messaging.[255] CTIA prescribes a requirement for express authorization prior to any collection activity other than those specific exceptions under Section 222 (d) & (f). As a matter of fact, it is of the opinion that express authorization may be made in written, oral, and electronic or other form under these principles so long

---

247 The Anti-Spamming Act, H.R. 718,107th Congress, 1st Session (2001); Section 5, (a) (2), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act, S. 630, 107th Congress, 21st Session (2001); and Section 4, The Unsolicited Commercial Electronic Mail Act, H.R. 95, 107th Congress, 1st Session (2001).

248 Section 5, (a) (5), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act, S. 630, 107th Congress, 21st Session (2001); Section 2 (a) (1), The Netizens Protection Act, H.R.3146, 107th Congress, 1st Session (2001); and Section 5 (a) (3), The Unsolicited Commercial Electronic Mail Act, H.R. 95, 107th Congress, 1st Session (2001).

249 *Id.*

250 The Wireless Telephone Spam Protection Act, H. R. 113, 107th Congress, 1st Session (2001).

251 *Id.* Section 2 (5) and Section 3 (a) (1) (e).

252 *1267632 Ontario Inc.* c. *Nexx Online Inc.*, Ontario Superior Court (July 9, 1999).

253 Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

254 *Id.* Article 12.

255 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 2.

as it manifestly evidences the customer's desire to participate in the location service or transaction.[256]

Please refer to Schedule "B" in order to view the Summarizing Chart on the legal framework relating to the choice and consent privacy issues.

2.3 Quality of the Data

According to the *OECD Guidelines,*[257] personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.[258]

In Europe, the *EC Directives*[259] also require that the collection of data must be adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed.[260] The data collected must be accurate and, where necessary, kept up to date and every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.[261] Finally, the data collected must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[262]

In the United States, the *Safe Harbor Agreement*[263] states that an organization must keep personal data relevant for the purposes for which it has been gathered only, consistent with the principles of notice

---

256 *Id.* CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 9.

257 OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980).

258 *Id.* Article 8.

259 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

260 Article 6 c), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

261 *Id.* Article 6 d).

262 *Id.* Article 6 e).

263 U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

and choice.[264] To the extent necessary for those purposes, the data should be accurate, complete, and current.[265]

In Canada, PIPEDA[266] mentions that personal information shall be as accurate, complete, and up to date as is necessary for the purposes for which it is to be used.[267] The extent to which personal information shall be accurate, complete, and up to date will depend upon the use of the information, taking into account the interests of the individual.[268]

In Quebec, the *Act Respecting the Protection of Personal Information in the Private Sector*[269] states that every person carrying on an enterprise must ensure that any file held on another person is up to date and accurate when used to make a decision in relation to the person concerned.[270]

MMA members creating, maintaining, using or disseminating PII should take reasonable steps to ensure that the data are accurate, complete, and timely for the purposes for which they are to be used.[271] This includes making reasonable efforts to ensure that they are obtaining data from reliable sources.[272] WLIA members collecting, using or disseminating geographically tagged PII must take appropriate measures to assure its accuracy.[273]

Please refer to Schedule "C" in order to view the Summarizing Chart on the legal framework relating to the data quality privacy issues.

---

264 *Id.* Article 5.

265 *Id.*

266 Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

267 *Id.* Schedule 1, Section 5, Article 4.6.

268 *Id.* Schedule 1, Section 5, Article 4.6.1.

269 Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

270 *Id.* Article 11.

271 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.waaglobal.org/ (Last accessed on July 8, 2002)

272 *Id.*

273 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

2.4 Security of the Data

According to the *OECD Guidelines*,[274] personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.[275]

In Europe, the *EC Directives*[276] states that the controller of the collected data must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.[277] This is especially important where the processing involves the transmission of data over a network and against all other unlawful forms of processing.[278] Having regard for the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.[279]

These Directives also provide, as a general rule, that telecommunication traffic data must be erased or made anonymous as soon as the communication ends.[280] This provision was motivated by the perceived sensitivity of traffic data revealing individual communication profiles including geographical locations of the user of wireless phones and the potential risks to privacy resulting from the collection, disclosure or further uses of such data. Two important exceptions to this rule allow for the processing of certain traffic data for the purpose of subscriber billing and interconnection payments, but only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.[281] It is interesting to note that these rules have been recently modified by the 2000 EC Proposal in order to enable LBS Provider to provide location-based services.

---

274 OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980).

275 *Id.* Article 11.

276 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

277 Article 17 1), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

278 *Id.*

279 *Id.*

280 Article 6 (1), Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

281 *Id.* Article 6 (2).

As a matter of fact, according to the 2000 EC Proposal, the provider of a publicly available electronic communications service may process the data for the purpose of marketing electronic communications services or for the provision of value-added services (or location-based services).[282] This may only be done for the duration necessary for such services or marketing, if the user to whom the data relate has given his consent.[283] Also, processing of traffic data and location data must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer inquiries, fraud detection, marketing electronic communications services or providing a value-added service.[284] This must further be restricted to what is necessary for the purposes of such activities.[285] In the case of location data, the processing is also possible by the third party providing the value-added service, but must be restricted to what is necessary for the purposes of providing such value-added service.[286] When location data can be processed, such data may only be processed when they are made anonymous or with the consent of the users.[287]

In the United States, the *Safe Harbor Agreement*[288] prescribes that the organizations creating, maintaining, using or disseminating records of personal information must take reasonable measures to assure its reliability for its intended use. [289] They must further take reasonable precautions to protect it from loss, misuse, unauthorized access or disclosure, alteration, or destruction.[290] The *Wireless Privacy Protection Act*[291] states that a customer shall not be considered to have granted express prior authorization for the collection of location data unless the carrier has established and maintains reasonable procedures to protect the confidentiality, security, and integrity of the information the

---

282 Article 6 (3), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

283 *Id.*

284 *Id.* Article 6 (5).

285 *Id.*

286 *Id.* Article 9 (3).

287 *Id.* Article 9 (1).

288 U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

289 *Id.* Article 4.

290 *Id.*

291 The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce

carrier collects. [292] Also the carrier shall maintain the data in accordance with such customer consents.[293] The *Location Privacy Protection Act*[294] mentions that the rules prescribed by the FCC shall ensure the security and integrity of location data[295] and require that aggregated location information[296] not be disaggregated through any means into individual location information for any commercial purpose.[297]

In Canada, PIPEDA[298] mentions that personal information shall be protected by security safeguards appropriate to the sensitivity of the information,[299] which shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.[300] Organizations shall protect personal information regardless of the format in which it is held[301] and the nature of the safeguards shall vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, as well as the method of storage.[302] As a matter of fact, PIPEDA suggests that more sensitive information should be safeguarded by a higher level of protection.[303] Finally, such law also prescribes that the methods of protection should include physical measures (for example, locked filing cabinets and restricted access to offices),[304] organizational measures (for example, security clearances and limited access on a *need-to-know* basis),[305] and technological measures, (for example, the use of passwords and encryption).[306]

(2001).

292 *Id.* Article (3).

293 *Id.*

294 The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

295 *Id.* Section 3, Article (b) (1) (D).

296 The term "aggregate location information" is defined as a collection of location data relating to a group or category of customers from which individual customer identities have been removed.

297 Section 3, Article (b) (1) (F), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

298 Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

299 *Id.* Schedule 1, Section 5, Article 4.7.

300 *Id.* Schedule 1, Section 5, Article 4.7.1.

301 *Id.*

302 *Id.* Schedule 1, Section 5, Article 4.7.2.

303 *Id.*

304 *Id.* Schedule 1, Section 5, Article 4.7.3.

305 *Id.*

306 *Id.*

In Quebec, the *Act Respecting the Protection of Personal Information in the Private Sector*[307] states that every person carrying on an enterprise who collects, holds, uses or communicates personal information about other persons must establish and apply such safety measures as are appropriate to ensure the confidentiality of the information.[308]

MMA is of the opinion that its members creating, maintaining, using or disseminating PII should take appropriate measures to assure the PII's reliability and should take reasonable precautions to protect it from loss, misuse, or alteration.[309]

The WLIA mentions that each WLIA member collecting, using, or disseminating geographically tagged PII must take appropriate measures to assure its accuracy and must take reasonable precautions to protect it from loss, misuse, unauthorized access, or alteration.[310] Furthermore, each WLIA member must take reasonable steps to ensure that third party recipients of such information are also made fully aware of these security practices and that the third parties will also take reasonable precautions to ensure the security of transferred information.[311] Each WLIA member shall avoid storing or maintaining records containing geographically tagged PII for any longer than necessary to accomplish the purpose for which such information is necessary.[312] Finally, CTIA is of the opinion that LBS Providers should maintain any location data collected securely.[313]

Please refer to Schedule "D" in order to view the Summarizing Chart on the legal framework relating to the data security privacy issues.

---

307 Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

308 *Id.* Article 10.

309 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 5.

310 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

311 *Id.*

312 *Id.*

313 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 10.

2.5 Transfer of the Data

In Europe, *EC Directives*[314] states that the data subject must have given his consent unambiguously to a proposed transfer.[315]

In the United States, the *Safe Harbor Agreement*[316] prescribes that individuals must be given the opportunity to choose whether, and the manner in which, a third party uses the personal information they provide and when such use is unrelated to the use(s) for which the individual originally disclosed it.[317] When transferring personal information to third parties, an organization must require that third parties provide at least the same level of privacy protection as originally chosen by the individual.[318]

The *Wireless Privacy Protection Act*[319] states that a customer shall not be considered to have granted express prior authorization unless the carrier has provided the customer in writing what information may be shared or sold to other companies and third parties.[320] The *Location Privacy Protection Act*[321] stipulates that the rules prescribed by the FCC shall require that all LBS Providers not subsequently release a customer's location data for any purpose beyond the purpose for which the customer initially provided express authorization.[322] Also, any third party receiving access to a wireless user's location data from a LBS Provider pursuant to such user's express authorization shall not disclose or permit access to such information to any other person without the express authorization of the user.[323]

---

314 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

315 Article 26 (a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

316 U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

317 *Id.* Article 3.

318 *Id.*

319 The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

320 *Id.* Article (1) (C).

321 The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

322 *Id.* Section 3, Article (b) (1) (C) (ii).

323 *Id.* Section 3, Article (b) (3).

The *Telecommunications Act of 1996*[324] included a new Section 222 to the *Communications Act of 1934.*[325] Such section enacts statutory restrictions on the use of CPNI (data regarding a customer's account and usage by carriers) and more specifically restricts the disclosure of CPNI to third parties, as well as the manner in which a carrier may use CPNI for the provision and marketing of its own services.[326] It may be interesting to note that the FCC was still until recently seeking new comments on customer consent for use of CPNI, including location data.[327]

In Canada, PIPEDA[328] mentions that care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.[329] In Quebec, the *Act Respecting the Protection of Personal Information in the Private Sector*[330] mentions that no person may communicate to a third person the personal information contained in a file he holds on another person.[331] Also, no person shall use such data for purposes not relevant to the object of the file, unless the person concerned consents thereto or such communication or use is provided for by this Act.[332] In the telecommunications sector, the policy objectives in Section 7 of the *Telecommunications Act*[333] are aiming to contribute to the protection of the privacy of persons. Since this restricts Canadian carriers, including cellular and Personal Communications Services providers (hereinafter **PCS**) from providing confidential customer information to third parties without the written consent of the customer, Bell Canada[334] and other companies applied to the Canadian Radio-

---

324 The Telecommunications Act § 47 U.S.C. § 222 Privacy of customer information (1996).

325 The Communications Act § 47 U.S.C. (1934).

326 Section 222 was again amended by the Wireless Communications and Public Safety Act of 1999, H.R., 106th Congress, 1st Session, on H.R. 438 & H.R. 514 (1999).

327 Wireless Location Industry Association, *FCC Seeks New Comments on Customer Consent for Use of Customer Proprietary Network Information (CPNI), including Location Data*, Newsletter, October 12, 2001. http://www.wliaonline.com/publications/fcccpni.html (Last accessed on July 8, 2002) and also see Before the Federal Communications Commission, Washington D.C., In the Matter of the Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, CC Docket 96-115 and 96-149, FEDERAL COMMUNICATION COMMISSION, Clarification order and second further notice of proposed rulemaking (September 7, 2001), 14 pages.

328 Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

329 *Id.* Schedule 1, Section 5, Article 4.7.5.

330 Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

331 *Id.* Article 13.

332 *Id.*

333 Section 7, Telecommunications Act, c. 38 (1993) (Canada).

334 Bell Canada provides a full range of communications services to customers, including wired and wireless local and long distance telephone services, Internet access, high-speed data services and directories. http://www.bell.ca/ (Last accessed on July 8, 2002)

television and Telecommunications Commission (hereinafter the **CRTC**)[335] in November 2000. They requested the CRTC to modify Article 11 of their Terms of Service in order to allow their affiliated companies to share confidential customer information without having to obtain written consent from the customer.[336]

MMA states that the permission of wireless users should not be transferable to third parties without explicit permission from such users.[337] WLIA members should also take steps to ensure that these privacy standards are adopted and/or made a condition of doing business with business partners, technology providers, and other partners.[338]

CTIA is of the opinion that systems employed by the LBS Providers should protect the location data of wireless users from both unauthorized access and disclosure to third parties.[339] CTIA further believes that, in the event that the wireless user authorizes such transfers to third parties, the LBS Provider should ensure that any third party to which location data is provided adheres to its location data privacy practices.[340]

Please refer to Schedule "E" in order to view the Summarizing Chart on the legal framework relating to the transfer of the data privacy issues.

---

335 The CRTC is an independent agency responsible for regulating Canada's broadcasting and telecommunications systems. http://www.crtc.gc.ca/ (Last accessed on July 8, 2002)

336 Bell Canada et al., *Application to Revise Article 11 of the Terms of Service*, Part VII Application to the CRTC. Ottawa (November 15, 2000), and Bell Canada et al., *Application to Revise Article 11 of the Terms of Service*, Public Notice CRTC 2001-60-1 (Ottawa, May 31, 2001). http://www.crtc.gc.ca/archive/eng/Notices/2001/PT2001-60-1.htm (Last accessed on July 8, 2002)

337 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 4.

338 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

339 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 10.

340 *Id.*

2.6 Access to the Data

According to the *OECD Guidelines*,[341] an individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him.[342] An individual shall also have the right to have communicated to him, data relating to him within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him.[343] Also, an individual should have the right to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.[344]

In Europe, the *EC Directives*[345] provide that the data collector must provide the data subject from whom data relating is collected the right to rectify the data concerning him.[346]

In the United States, the *Safe Harbor Agreement*[347] mentions that individuals must have reasonable access to information about them derived from non-public records that an organization holds, and be able to correct or amend that information when it is inaccurate.[348] Such Agreement also mentions that reasonableness of access depends on the nature and sensitivity of the information collected and its intended uses.[349] The *Location Privacy Protection Act*[350] mentions that wireless users should have reasonable access to their location data for purposes of verifying the accuracy of, or deleting, such data.[351]

---

341 OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980).

342 *Id.* Article 13 a).

343 *Id.* Article 13 b).

344 *Id.* Article 13 d).

345 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

346 Article 10 c), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

347 U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

348 *Id.* Article 6.

349 *Id.*

350 The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

351 *Id.* Section 3, Article (b) (1) (D).

In Canada, PIPEDA[352] mentions that upon request, an individual shall be given access to his collected information and shall be able to challenge the accuracy and completeness of such information and have it amended as appropriate.[353] In Quebec, the *Act Respecting the Protection of Personal Information in the Private Sector*[354] states that any person holding personal information on behalf of a person carrying on an enterprise may refer to the latter every request for access or rectification received from a person to whom such information relates.[355]

On the industry side, MMA members should establish appropriate processes or mechanisms so that inaccuracies in PII, such as account or contact information, may be corrected.[356] These processes and mechanisms for access should be simple and easy to use, and provide assurance that inaccuracies have been corrected.[357] The MMA also recommends that members honor requests from wireless users to delete their PII in the event they change carriers or devices or simply unsubscribe from the service.[358]

The WLIA prescribes that each of its member shall honor requests from wireless users to remove, where possible and permitted by law, their geographically tagged PII in the event they terminate their subscriptions to the WLIA member's service.[359] CTIA states, in the case where the LBS Provider maintains location data as part of a customer profile, that it would support reasonable customer access to the profile to correct any inaccuracies, similar to the access provided to other call detail records.[360]

Please refer to Schedule "F" in order to view the Summarizing Chart on the legal framework relating to data access privacy issues.

---

352 Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

353 *Id.* Schedule 1, Section 5, Article 4.9.

354 Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

355 *Id.* Article 16.

356 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 5.

357 *Id.*

358 *Id.*

359 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

360 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR

3 Tracking Technology and Privacy Issues

The uncontrolled availability of location data and possibility of wireless spam present serious risks to individual privacy. As a matter of fact, most wireless users carry their wireless phones round the clock. Also, LBS Providers need to respect the wireless users' rights to decline receiving messages.

Current wireless phones can pinpoint wireless users from a few kilometers to a few meters by determining the location of the cell tower used to handle the call. Other location services are based on knowing the position of existing fixed reference points and then relating these to the location of the device that is *lost.* Some common examples of reference points are the GPS satellites and the cellular base stations.

With its tracking capabilities, wireless phones may compromise the personal privacy of users in two ways:

- The first way is related to the tracking, where the problem is that, over time, historical location data collected and stored in databases will enable a LBS Provider or a third party to build a very detailed and invasive dossier of a wireless user's travel patterns, movements, and other habits. The continuous tracking capability could virtually eliminate an individual's capacity to move freely without surveillance. Without some way for wireless users to control being tracked, users may fear they will be monitored without restriction. If the location data is stored, location tracking could result in a 24-hour-a-day record of a person's whereabouts.[361]

- The second way is related to the real-time location data that would be used to send messages to the wireless user, supposedly at the right tiem and place to make the message relevant, which would be very intrusive in the event that such message is unanticipated by the user.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 10.

361 Cnn.com, *Internet Devices coming that reveal your location*, October 30, 2000.
http://www.cnn.com/2000/TECH/computing/10/30/wireless.tracking.ap/ (Last accessed on July 8, 2002)

On these privacy issues and as previously mentioned, Windwire[362] executed a national trial of wireless advertising in the United States in the Fall of 2000 where millions of wireless ads were delivered to wireless users who access their favorite web content using phones and PDAs. Their report was published in December of 2000 and stated that, according to their study, sixty-four percent (64%) of participants were concerned with privacy issues[363] and with regards to *push* location-based advertising in particular.[364]

If a company is collecting and bringing together all that type of information, they will know a lot about the consumer. For example, Gartner[365] believes that such company would know the consumer's habits, where they are, whom they are with and what they are doing at any point in time.[366]

Mark Lemaitre from Nextel[367] pointed out the fact that consumers will have a hard time giving out information about their personal movements:

> One of the things that we found was that -- or discussed was that in order to make the experience a lot more compelling in a wireless environment, certainly with the PDA, the notion of where I am and what I'm doing becomes extremely important, and so whilst I agree that protocols that we have got on the -- being developed on the Internet today for privacy satisfy the notion that I'm in front of a big screen surfing content, when I get into a wireless environment, the stakes go up in that I've now got information about my personal location, my personal --you know, my state, what am I doing. What am I doing and where am I doing it are very difficult things for people to give away easily, and I'm wondering if you can just touch, Danny, on the notion that as the stakes go up, so do the controls, and the levers that we have to put back in the consumers' hands have to get better.[368]

---

362 Windwire has developed a technology that allows advertisers to deliver targeted offers for each consumer's wireless device. http://www.windwire.com/ (Last accessed on July 8, 2002)

363 Windwire Inc., *First-to-Wireless: Capabilities and Benefits of Wireless Marketing and Advertising Based on the First National Mobile Marketing Trial*, December 27, 2000, p. 24.

364 *Id.*

365 Gartner Inc. is a research and advisory firm. http://www.gartner.com/ (Last accessed on July 8, 2002)

366 Adam Daum, *The Mobile Consumer*, GARTNER INC., Symposium ITxpo 2000, Orlando, Florida, October 2000, p. 13.

367 http://www.nextel.com/ (Last accessed on July 8, 2002)

368 Mark Lemaitre, Nextel Communications, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 11, 2000, p. 18. http://www.ftc.gov/bcp/workshops/wireless/001211.htm (Last accessed on July 8, 2002)

The present laws, which may apply to the protection of the privacy of wireless users in the case of personalized location-based services, are the laws regarding the protection of personal data and the laws prohibiting spam. Laws may be important when we are talking about issues like enforcement but one main problem is that laws are different in many countries and among many states in the U.S. This is a problem when we are talking about these types of location-specific services that are usually deployed on a large scale, if not globally.

On this issue, in its comments produced in the context of a CTIA Petition, carrier Sprint PCS[369] was stating that the rules regarding privacy in the context of location-based services should be national, if not global, in scope.[370] As a matter of fact, since disparate laws are not workable for wireless users or carriers, state laws in this area must be preempted. XNSORG[371] in its comments also noted that there could be problems that disparate country laws would pose for global roamers. It further discussed how the privacy laws in one country could often impact other foreign jurisdictions since cross-jurisdictional variations in privacy legislation are already causing many U.S. companies considerable difficulties as they seek to operate within the European Union. Sprint PCS[372] submitted that the problem is larger and even more serious than what XNSORG[373] describes and stated the following:

> The Internet does not conform to country boundaries. Thus location information concerning U.S. citizen can be accessed (or transferred), used and stored by applications service providers ("ASPs") located outside the United States. Will U.S. privacy laws reach foreign-based ASPs? Will U.S. regulatory authorities possess the authority and resources to seek sanctions against foreign-based ASPs that misuse the location data of U.S. citizens? What recourse will U.S. citizens have for a breach of their privacy rights? Must they file a lawsuit in the foreign country, effectively insulating the ASP from liability?[374]

---

369 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

370 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Reply to Comments (April 24, 2001), 16 pages, p. ii.

371 The XNS Public Trust Organization manages the widespread acceptance of eXtensible Name Service (XNS) as an open, independent infrastructure for Web identity. http://xns.org/ (Last accessed on July 8, 2002)

372 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

373 http://xns.org/ (Last accessed on July 8, 2002)

374 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Reply to Comments (April 24, 2001), 16 pages, p. 3.

Also, it is to be considered that wireless users will be confused if they encounter different notices and consent screens as they travel from one jurisdiction to another. Understandably, they will further be upset if they cannot obtain desired services in certain areas because of peculiar requirements adopted in certain states.[375]

Furthermore, we may want to take into account the fact that rules were written in a very general language and were designed to protect personal information collected through a traditional way. As a matter of fact, author Robert Gellman in his article entitled: *Does Privacy Law Work?* was criticizing the vagueness of the present rules. He states that "personal data should be relevant to the purposes for which they are to be used and should be accurate, complete, and timely" taken from the *EC Directive* on privacy is extremely vague.[376] Author Victoria Bellotti was outlining, in her article entitled: *Design for Privacy in Multimedia Computing and Communications Environments* that:

> If the law is so complex and unintuitive, then it seems that no team of designers, consultants, and users, or anyone else for that matter, is likely to be able to agree upon who should have access to whom or what in which circumstances.[377]

For this reason, not only is it to be determined if the present legal framework actually applies to location data, as further discussed in the introduction of Section 2, but we have to consider that, even if such framework does apply, it is often vague regarding certain issues and incomplete with regards to others. The framework does not take into account the issues resulting from the collection of this new type of data for the purpose of providing personalized location-based services through wireless devices.

Also, not only are these laws not very specific, but they also have different views on certain issues such as the time when the disclosure should be made. They do not take into consideration the specific nature of a location-based service and the issues surrounding it, like the size of the screen of the device and the specifics of the main players involved in the providing of this new type of service.

---

375 *Id.* Comment, April 6, 2001, 25 pages, p. 19.

376 Robert Gellman, *Does Privacy Law work?*, Technology and Privacy: The New Landscape, edited by Philip E. Agre and Marc Rotenberg, MIT Press, 1998, p. 193, p. 197.

377 Victoria Bellotti, *Design for Privacy in Multimedia Computing and Communications Environments*, Technology and Privacy: The New Landscape, edited by Philip E. Agre and Marc Rotenberg, MIT Press, 1998, p. 63, p. 67

An analysis of all of the actual standards, laws and regulations as well as the specific issues relating to this new type of service may help to determine how the appropriate system should be built and what would be the appropriate business model adopted by LBS Providers. Such system should enable a LBS Provider to gather location data and provide for a range of systems that would provide consumer convenience but avoid some of the surveillance, tracking, and record-keeping problems.

For these reasons, a LBS Provider looking to deploy location-based services as of today should take into account the following issues that are not clearly addressed in the current legal framework. These issues are related to the disclosure to be given and the consent to be obtained from the wireless user prior to the tracking and the providing of location-based services. Such issues also cover the quality of the collected data, the security of such data, and the transfer of-- and the access to--the said data.

3.1 Effective and Full Disclosure

The disclosure (also known as *notice* or *privacy policy*) is the most fundamental of all principles. Without an appropriate and effective disclosure, a wireless user cannot make an informed decision as to whether, and to what extent, to disclose personal information or to agree to being tracked, and whether he wishes to receive location-based services. According to Howard Beales, Director at the FTC's Bureau of Consumer Protection,[378] privacy notices should be viewed as a means of facilitating competition over privacy practices.[379] Their goal should be to help consumers understand what information is collected about them and what is done with that information, not to simply scare consumers into opting-out of information sharing.[380]

In the specific context of location-based services, disclosure is the notice to the wireless user of the tracking and the collection of his personal or location data that will take place and related issues, regardless of whether messages will be sent to such user.

---

378 The Bureau of Consumer Protection is part of the FTC and its mandate is to protect consumers against unfair, deceptive, or fraudulent practices. http://www.ftc.gov/bcp/bcp.htm (Last accessed on July 8, 2002)

379 Howard Beales, Director, Bureau of Consumer Protection (Federal Trade Commission), *Privacy Notices and the Federal Trade Commission's 2002 Privacy Agenda*, Remarks, January 24, 2002. http://www.ftc.gov/speeches/other/privacynotices.htm (Last accessed on July 8, 2002)

380 *Id.*

In today's wireless communications networks, location data giving the geographic position of wireless users (or, strictly speaking, that of their terminal equipment) already exist. This information is necessary to enable the transmission of communications from and to a user without a fixed location and current wireless device networks can locate a user based on the closest cell phone tower, to within a distance ranging from several hundred meters to kilometers.[381] For this reason, it is not clear if it would be appropriate to even disclose to the wireless user that he will be tracked, considering the fact that the network already knows where the user is today.

The present laws and regulations provide, in a general way, the legal framework to enable LBS Providers to disclose the purpose of the location data collection prior to such collection or use of the data. At the same time, the complete details surrounding the disclosure to ensure that it is effective in the context of location-based services have never been addressed and clearly defined. Also, in most cases one law may be more specific to one disclosure issue but fail to address another important one. For this reason, an analysis of each of the issues surrounding the disclosure in the context of the provision of location-based services will follow.

3.1.1 Who Should Be Provided with the Disclosure?

In a general way, the North American and European laws and regulations further analyzed under Subsection 2.1 mention that the disclosure should be made to the subject prior to the data collection[382] or the usage or processing of such data.[383]

These laws do not specify whether the tracking should be disclosed only to the users who have agreed to receive messages, to any wireless user being tracked, or whether the tracking should also be disclosed to a wireless user being tracked on an anonymous basis.

---

381 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, p. 3.

382 Article 9, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 1, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); and Schedule 1, Section 5, Article 4.2, and Articles 5 (3) and 7, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

383 Article (1) (B), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

3.1.1.1 Status of Anonymous Location Data

If there is PII associated with location data, it clearly becomes personal data. In such case regulations regarding the protection of personal data provide that the consent of the wireless user be obtained prior to either the collection or the use of such data. The next issue is: Should the wireless user be provided with a disclosure prior to being tracked on an anonymous basis?

There seems to be a different status for anonymous tracking. For example, companies like Intelligent Transportation Society of America[384] in the United States have requested that the FCC[385] make a distinction between location tracking and anonymous location tracking. The purpose of such request is so that it is able to move forward with its business without having to disclose anything to the wireless users that it is tracking anonymously. It claims that the collection of this type of data has the potential to provide traffic engineers and planners with rich data feeds necessary to promote optimal traffic flows, to efficiently allocate transportation resources, and to properly reroute traffic in emergency situations.[386]

The *Location Privacy Protection Act* introduced in the U.S. Senate in July 2001 makes a distinction and treats anonymous location data differently than location data that would include PII. As a matter of fact, such Act mentions that the collection, use, retention, disclosure of, or access to a customer's location information without prior notice or consent of the wireless user is acceptable to the extent necessary to produce *aggregate location information*.[387] This term is further defined as the collection of location data relating to a group or category of customers from which individual customer identities have been removed.[388] This seems to imply that a LBS Provider may collect and use the anonymous location data without informing wireless users that it is tracking them.

---

384 Public/private partnership serving as a utilized Federal Advisory Committee to the U.S. Department of Transportation, Educational and scientific research organization created in 1991 for the purpose of fostering the development and deployment of intelligent transportation systems.

385 http://www.fcc.gov/ (Last accessed on July 8, 2002)

386 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, INTELLIGENT TRANSPORTATION SOCIETY OF AMERICA, Reply Comments (April 24, 2001), 16 pages, p. 7.

387 Section 3, Article (b) (2) (D), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

388 *Id.* Section 3, Article (f) (1).

Also, the 2000 EC Proposal mentions that where location data can be processed, such data may only be processed when they are made anonymous (unless the user provides his consent to the processing), therefore providing for a different treatment for such type of anonymous data.[389]

To this day, the FCC is trying to determine the notion of customer consent for use of CPNI, including location data.[390] For this reason, it is still to be determined if a carrier or a LBS Provider may collect and process this anonymous location data without disclosing it to the wireless user.

3.1.1.2 Ownership of Location Data

Before determining who should be provided with the disclosure relating to the location-based services, we need to determine who owns and control this location data, which debate is one of the most critical issues facing the information economy.[391]

As a matter of fact, if we consider that the carrier owns this data, he (or the LBS Provider with whom he is partnering) may not have to provide wireless users the disclosure relating to the collection of their location data. At the same time, if we consider that wireless users own this data, they should be provided with the disclosure prior to any collection of such data.

The issue of the ownership of the wireless user's location data is a highly controversial issue created by these new tracking technologies as was outlined by Gartner in an article on privacy.[392] Also, a news article from author Matt Hamblen from Computerworld entitled: *Ensuring portable privacy - Banks, retailers and airlines face the opt-in issue and other challenge* refers to John Pescatore's

---

389 Article 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

390 Wireless Location Industry Association, *FCC Seeks New Comments on Customer Consent for Use of Customer Proprietary Network Information (CPNI), including Location Data*, Newsletter, October 12, 2001. http://www.wliaonline.com/publications/fcccpni.html (Last accessed on July 8, 2002) and also see Before the Federal Communications Commission, Washington D.C., In the Matter of the Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, CC Docket 96-115 and 96-149, FEDERAL COMMUNICATION COMMISSION, Clarification order and second further notice of proposed rulemaking (September 7, 2001), 14 pages.

391 Arabella Hallawell, *Mr. President, It's time for New Privacy Protection methods*, GARTNER INC., Research Note, March 1, 2001, p. 1.

392 Arabella Hallawell, *Beyond the Headlines: Privacy Issues and the Enterprise*, GARTNER INC., May 4, 2001.

statement, an analyst at Gartner and confirms the controversy of this issue:

> A consumer theoretically could say whether he wants his location kept secret or not when he signs up for a wireless service, but the real question is who owns that location information? It's not clear.[393]

This issue has also been raised by Michael Amarosa, VP Public Affairs at TruePosition:[394]

> There's been a lot of talk that the carriers own the location part of the data and what's coming over their network. I think these are things still open to discussion at this point.[395]

Forrester Research was also wondering who was the owner of a consumer's location data, whether if it was the person carrying a phone or the operator who was provisioning it.[396]

SiRf[397] has endorsed the same view as the Location Privacy Association,[398] which strongly believes that the wireless user is the sole owner of his location data.[399] Goldman Sachs[400] has stated that while the winners are unclear, much will depend on who is best positioned in the minds of customers today.[401]

It is still unclear at this point who owns the location data of the wireless user. Should it be the wireless user, the carrier or the LBS Provider? More specifically, how does that play into the control of the location data?

---

393 Matt Hamblen, *Ensuring portable privacy - Banks, retailers and airlines face the 'opt-in' issue and other challenges*, COMPUTERWORLD, December 11, 2000. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO54794,00.html (Last accessed on July 8, 2002)

394 TruePosition technology locates wireless phones, enabling wireless carriers to provide E-911 and other location-based services to wireless users around the world. http://www.trueposition.com/ (Last accessed on July 8, 2002)

395 Michael Amarosa, VP Public Affairs, True Position Inc., participant at the Federal Trade Commission – Panel on generation and control of location information, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 28. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

396 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, p. 17.

397 SiRF Technology Inc. is a leader in GPS Enabled Location Technologies. http://www.sirf.com/ (Last accessed on July 8, 2002)

398 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, LOCATION PRIVACY ASSOCIATION, Comment (April 6, 2001), 18 pages, p. 4.

399 *Id.* SIRF TECHNOLOGY INC., Notice (April 30, 2001), 14 pages, p. 12.

400 Goldman Sachs is a global investment banking and securities firm. http://www.gs.com/ (Last accessed on July 8, 2002)

401 Goldman Sachs, *Technology: Mobile Internet*, MOBILE INTERNET PRIMER, July 14, 2000, p. 1.

3.1.2 Who Should be Responsible for Providing the Disclosure?

The legal framework analyzed under Subsection 2.1 mentions that the data collector should make the disclosure without specifying, in the case of location-based services, to which party in the value chain we are referring.

As a matter of fact, one of the main issues related to the disclosure is which party should be in charge of providing the disclosure relating to the tracking of the wireless users. For example, should it be the LBS Provider who actually deploys the location-based service? Should it be the wireless device manufacturer, the carrier that already provides telecommunication services to its subscribers and that may play the role of the data collector in many cases, the advertisers and content providers, or all of the above? At no time do the laws and regulations actually consider the types of relationships that the wireless user will have with all and every party involved in this value chain. Danny Weitzner from the World Wide Web consortium[402] was raising the issue of which party should be trusted:

> (...) who is the user going to trust in these sorts of situations? The carrier is the source maybe of that location or maybe it's some other entity in the network that knows your location. Who is the user going to rely on to mediate in some sense the disclosure of that information to make sure that as it's used in various other parts of the network, it's used consistent with the desire of the user (...)[403]

Dana Rosenfeld, Office of Director at the Bureau of Consumer Protection,[404] raised this issue of which parties were in the best position to provide notice and choice.[405] To this question, Alan Davidson, attorney for the CDT answered that he thought it was going to be all of the above.[406] Also,

---

402 The World Wide Web Consortium (W3C) develops interoperable technologies for the Internet. http://www.w3.org/ (Last accessed on July 8, 2002)

403 Danny Weitzner, World Wide Web consortium, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues, Wireless Web Workshop*, December 11, 2000, p. 18. http://www.ftc.gov/bcp/workshops/wireless/001211.htm (Last accessed on July 8, 2002)

404 http://www.ftc.gov/bcp/bcp.htm (Last accessed on July 8, 2002)

405 Dana Rosenfeld, Office of Director at the Bureau of Consumer Protection, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 9. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

406 Alan Davidson, attorney, Center for Democracy and Technology, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 9.

Donald Bromley from Fiderus Strategic Security and Privacy Services[407] shared the FTC and CDT views that each party involved in providing location-based services should also be involved in providing the confidence to the wireless user that the collected data is protected:

> It's a chain of confidence that has to happen so that every party has to be involved from the handset manufacturers to the carriers to your -- to the service providers and the ASPs and every party involved in that transaction has to provide that confidence that that information is being protected and used for appropriate purposes based on the consumer's choice.[408]

This position that the disclosure should come from all of the parties may not be a very practical one given that this may require too much coordination between the wireless device manufacturer, the carrier, the LBS Provider, and the content provider. This would most likely confuse the wireless user more than anything, especially in the event that they each have their own privacy policies.

3.1.3 How Should the Disclosure be Given?

The law generally takes the position that the method chosen to make a disclosure depends on the nature of the business[409] and other considerations and that, depending upon the way in which the information is collected, the disclosure can be done orally or in writing.[410] The legal framework further provides that the disclosure be done in clear and conspicuous language,[411] in a way easy to find and understand,[412] perhaps accessible with a service contract,[413] through an application form,[414]

---

http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

407 http://www.fiderus.com/ (Last accessed on July 30, 2001)

408 Donald Bromley, Fiderus Strategic Security and Privacy Services, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 10. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

409 Schedule 1, Section 5, Article 4.8.3, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

410 *Id.* Schedule 1, Section 5, and Article (1) (A), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

411 Article 1, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); and Section 3, Article (b) (1) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

412 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

413 *Id.*

414 Schedule 1, Section 5, Article 4.2.3, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

or simply available on websites.[415] The *WLIA Privacy Policy Standard* further suggests that such disclosure be done on wireless devices, when technically feasible.[416]

Such framework never considers the fact that the wireless device has unique characteristics, in contrast to desktop computers, which include the relatively small screen sizes of these wireless devices. This characteristic limits the ability of carriers or LBS Providers to provide a privacy notice or a disclosure directly to the hand-held device.

With regards to this issue, Lawrence Ponemon from Pricewaterhouse,[417] has also outlined this problem, raising the fact that a LBS Provider may have a hard time making an effective disclosure on the small screen of a wireless device:

> This is a great telephone, but look at the screen. Can you see it? I can't even see it. How do I know the privacy policy of a site that I'm visiting, okay? Some telephones have a larger screen, so you could actually build it out so you have eight lines, four lines, but it becomes pretty difficult from a pure mechanical point of view basically to use this to understand the full issue. I mean, it's difficult enough when you're basically looking at an Internet site in the wired Internet, right, to be able to understand what a privacy policy states. So I think we have to rely on other mechanisms.[418]

There may be a better way for LBS Providers than to make their disclosure on the wireless device screen, especially given that most of the wireless phones on the market only have the capability of containing 160 characters. But what is the appropriate way? On this issue, Wireless Consumers Alliance[419] states that a disclosure should not be considered appropriate if buried in other documents or letters or in the event that the wireless user had to undertake steps to learn of the invasion of his privacy.[420]

---

415 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

416 *Id.*

417 http://www.pwcglobal.com/ (Last accessed on July 8, 2002)

418 Lawrence Ponemon, Pricewaterhouse, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues, Wireless Web Workshop*, December 12, 2000, p. 6. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

419 Wireless Consumers Alliance Inc. is an independent, non-profit organization which was formed to promote and serve the interests of consumers of wireless services in the United-States. http://www.wireless-consumers.org/ (Last accessed on July 8, 2002)

420 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS CONSUMERS

Also, and on a more general note, according to the FTC, the most extensive experience in the United States to date with privacy notices has been under the Gramm Leach Bliley Act[421] (hereinafter the **GLB**), which requires notices to be sent out annually by a broadly defined group of financial institutions. It is estimated that more than a billion notices were sent out in the first year under this Act. In late 2001, the FTC and the seven federal financial regulatory agencies charged with implementation of the statute held and hosted a workshop entitled: *Get Noticed* to explore initial experiences under the GLB notice provisions (hereinafter the **Get Noticed FTC Workshop**).[422]

Some of the findings of the Get Noticed FTC Workshop endorsed the fact that more privacy notices were not necessarily better and that adding additional notices and forms to those consumers are now receiving was unlikely to help.[423] As a matter of fact, it appears that many consumers are already confused and that multiple forms and notices are unlikely to improve the situation.[424] Secondly, rigidly prescribed disclosure formats were found not to be the answer and it was found that the experience with GLB notices revealed that many of them were hard to read, comprehend, and act on and that carefully researched standardized forms had proven useful.[425]

It is also vital that standard form disclosure requirements not impede the industry's ability to evolve. As a matter of fact, it was also discussed at the Get Noticed FTC Workshop that the one-size-fits-all approach to privacy notices also risks homogenizing privacy choices, rather than differentiating firms that truly excel at providing privacy.[426] Also, a standard form adopted today, cannot possibly foresee all of the changes in technologies or new types of services that are likely to appear in the near future and that will modify the type of disclosure appropriate and related to such changes, much less accommodate them all.

ALLIANCE INC.,Comment (April 6, 2001), 8 pages, p. 2.

421 The Gramm-Leach-Bliley Act § 15 U.S.C. §6803 (2001).

422 Public Workshop on Financial Privacy Notices, 66 Fed. Reg. 49742 (2001). http://www.ftc.gov/bcp/workshops/glb/ (Last accessed on July 8, 2002)

423 Howard Beales, Director, Bureau of Consumer Protection (Federal Trade Commission), *Privacy Notices and the Federal Trade Commission's 2002 Privacy Agenda*, Remarks, January 24, 2002. http://www.ftc.gov/speeches/other/privacynotices.htm (Last accessed on July 8, 2002)

424 *Id.*

425 *Id.*

426 *Id.*

3.1.4 When Should the Disclosure be Given?

The time when the disclosure should be given to the wireless user is an important issue. The present laws do not seem to agree on when the disclosure should take place. Some laws will promote that the disclosure take place prior to the collection of data,[427] while others promote that the disclosure take place prior to obtaining the consent of the user for the location-based service[428] or prior to the use of such collected data.[429]

The CTIA,[430] the main trade association for wireless companies in the United States, seems to be agreeing with the position that the LBS Providers should inform the wireless user about the specific location data collection[431] and use practices before any use of the location data takes place.[432] From a more practical point of view, it should be determined if, for example, the disclosure should be provided when a phone is sold or later, perhaps over a desktop computer hooked up to the Internet.

3.1.5 What Should be the Content of the Disclosure?

In a general way, the laws and regulations analyzed under Subsection 2.1, with regards to the content of the disclosure, may specify certain information that needs to be disclosed, while omitting to mention other important information that should also be part of the disclosure. None of the laws

---

427 Article 9, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 1, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Schedule 1, Section 5, Article 4.2, and Articles 5 (3) and 7 Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

428 Articles 6 (4) and 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

429 Article (1) (B), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

430 http://www.wow-com.com/ (Last accessed on July 8, 2002)

431 By "collection", CTIA means the acquisition of location information other than that used to complete a call or provide a subscriber access to a network. In most wireless systems, a user's rough location (i.e., the nearest cell site) is known to the network and is an integral part of completing wireless calls. This is not considered "collection" activity according to CTIA: See Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 9.

432 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR

analyzed were complete with regards to information that should be covered in an effective disclosure. This information should include whether the wireless user is simply informed when location data is collected, why is tracking being used, what type of tracking technology is used, how long the location data will be stored, who will have access to it, etc.

AT&T Wireless has recently posted its privacy policy on its website.[433] It has done a great job at drafting a privacy policy that is easily available and user-friendly, since in plain language it clearly explains how it intends to safeguard the collected data with specific security measures. However, such policy, if only analyzed in the context of providing location-based services, would not be sufficient. For example, the said policy states, relating to the collection and use of location data, that "we will use this information for additional services only if you have given us your express prior authorization to do so" without specifying the way of obtaining the user's consent. Also, the said policy is not clear as to what steps are undertaken by AT&T wireless to ensure that they are collecting quality location data or the mechanism used to provide access by the wireless user to the collected location data in a form that is eligible to the user. Furthermore, and relating to the update of the policy, AT&T states the following:

> AT&T Wireless will revise or update this Policy if our practices change, as we change existing or add new services or as we develop better ways to inform you of products we think will be of interest. You should refer back to this page often for the latest information and the effective date of any changes. If, however, users' personally identifiable information will be used in a manner materially different from that stated at the time of collection we will notify users via posting on this page for 30 days before the material change is made. Users will have a choice as to whether or not their information will be used in this materially different manner.[434]

The Ontario Superior Court of Justice has recently ruled in *Kanitz v. Rogers Cable Inc.*[435] that such procedure of notifying changes to a privacy policy via web posting was adequate. In this case, the court stayed a class action suit against Rogers Cable by concluding that a clause added to a user agreement, which mandated that all disputes had to be referred to arbitration to the exclusion of the

---

TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 9.

433 AT&T Wireless, *AT&T Wireless Privacy Policy*, Effective February 7, 2002. http://www.attws.com/privacy/ (Last accessed on July 8, 2002)

434 Section entitled: "Updating this Policy", *AT&T Wireless Privacy Policy*, Effective February 7, 2002. http://www.attws.com/privacy/ (Last accessed on July 8, 2002)

435 *Kanitz* v. *Rogers Cable Inc.*, Docket 01-CV-214404CP, Ontario Superior Court (February 22, 2002).

courts, was a valid arbitration agreement. The original user agreement stated that amendments to the agreement could be made at any time, with notice to customers on Rogers' website. Rogers subsequently amended the agreement, adding the arbitration clause and posting notice of it on the Rogers customer support website. The plaintiffs submitted that they were given inadequate notice of the amendment, because the process of finding the user agreement on the website was unduly cumbersome and because the amendment was buried in the agreement. The court found that the evidence did not support the plaintiffs' assertions, as it took a review of only five screens on Rogers' website to get to the user agreement. With respect to the clause being buried, the court found that it was no more difficult to read than any other term of the agreement, and that scrolling was no different from turning pages in a written document.

Notwithstanding this unusual judgment, the procedure requiring that the wireless user refers back to the privacy policy web page *often* (or at least every thirty (30) days) to ensure that their PII will not be used in a manner materially different from that stated at the time of collection is burdensome and inappropriate. A wireless user who has agreed to the collection and processing of his personal or location data for obtaining a certain service should not be required to follow up with the privacy policy of the collector of the information. Furthermore such user should be conversant on how the data collector intends to inform him of any change related to its privacy policy, as will be further detailed under Subsection 4.1.5.

3.2 Choice and Consent

Dana Rosenfeld, Office of Director at the Bureau of Consumer Protection,[436] raised the issue *How should choice be provided and who should provide it?*[437] in the context of location-based services. There are many privacy issues related to consent and when we raise the *consent* issue, we are talking about many things. First, we are talking about the consent of the user to being tracked. Within this issue, there is a distinction to be made between people who are being tracked for the purpose of being provided with push location-based services, people who are being tracked with the knowledge from the data collector of their identity, and people who are being tracked on an anonymous basis.

---

436 http://www.ftc.gov/bcp/bcp.htm (Last accessed on July 8, 2002)

437 Dana Rosenfeld, Office of Director at the Bureau of Consumer Protection, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12,

Also, consent may have to be given not only prior to the tracking of the wireless user, but also prior to sending messages to the user on a *push* basis in order to avoid spam-related issues. In that context, this last type of consent implies many other things like the type and frequency of advertising messages a wireless user has agreed to receive.

Mike Gurski, Senior Technology Advisor for the Ontario Information and Privacy Commission[438] was raising in his report entitled: *Privacy in the Wireless World*[439] one of the most problematic privacy issues facing the wireless world, which is the notion of *meaningful consent* related to a location-based service:

> Some have argued that as long as consumers consent to the collection, use, and disclosure of personal information through wireless technologies, the privacy issue can be easily resolved. In order for consent to meaningful, however, it must be *informed.* This is becoming increasingly difficult as technology outstrips the guidelines that govern it.[440]

Although the laws and regulations are clear on the fact that the wireless user's consent is needed prior to using the collected location data and pushing messages to wireless devices, they do not specify other important issues. Such issues include from whom the consent should be taken and which party should be in charge of obtaining such consent. Also, the laws are not unanimous on the way (opt-in versus opt-out procedure) and the time to obtain such consent. Finally, they are not clear on what the content of an appropriate and meaningful consent should be in the context of location-based services.

3.2.1 From Whom do you Get the Consent?

It may be obvious that it will be necessary to obtain the consent from the wireless users prior to sending location-based messages in order to avoid spam. But should a LBS Provider also obtain the consent from a wireless user that will be tracked, or that will be tracked on an anonymous basis? On

---

2000, p. 9. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

438 http://www.ipc.on.ca/ (Last accessed on July 8, 2002)

439 Mike Gurski and Ann Cavoukian, *Privacy in the Wireless World*, Ontario Information and Privacy Commission, July 25, 2001.

440 *Id.* p. 3.

this last issue, Nextel Communications[441] pointed out the fact that there should be a distinction made for wireless users tracked anonymously.[442] They further stated that the statutory requirements for *customer express prior authorization* and the foregoing location information policy guidelines should not apply to the collection of location data (as opposed to the use, access or disclosure of such information) as well as to the treatment of non-PII aggregate customer information.[443] For this reason, and for reasons further detailed under Subsection 3.1.1.1, it is to be determined that a LBS Provider may collect and process this anonymous location data without first obtaining the wireless user's consent.

Also, before determining from whom the LBS Provider should obtain the consent, we need to determine who owns and controls this location data, as further detailed under Subsection 3.1.1.2. As a matter of fact, if the carrier owns the location data, it may not have to obtain the wireless user's consent prior to collecting and processing such data, whether anonymous or not.

3.2.2 Who should be Responsible for Obtaining the Wireless User's Consent?

Lawrence Ponemon from Pricewaterhouse[444] has raised the following and legitimate issue:

> And there would be different touch points with the consumer, the device manufacturer, the carrier, the ad serving company. All of these people will be touch points so when you opt-in or opt-out or whatever, when you express choice, who is honoring that and how can you test, how can you verify that that touch point is honoring that commitment?[445]

It may make the most sense to have the party that will be providing the disclosure to the wireless user also obtain the wireless user's consent in order to avoid any potential confusion from the part of the user. At the same time, this would also enable the wireless user to know who is his primary contact

---

441 http://www.nextel.com/ (Last accessed on July 8, 2002)

442 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, NEXTEL COMMUNICATIONS INC., Notice (May 14, 2001), 7 pages, p. 2.

443 *Id.*

444 http://www.pwcglobal.com/ (Last accessed on July 8, 2002)

445 Lawrence Ponemon, Pricewaterhouse, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 6. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

for anything related to the location-based service.

3.2.3 How Should the Consent be Obtained?

The next issue is what is the appropriate way to obtain such consent from the wireless user in order to ensure that he gave his consent in a meaningful manner. For example, certain laws or industry players mention that it should be done in writing,[446] while others promote that it may be done orally[447] or through technological mechanisms.[448] Furthermore, PIPEDA suggests that the form of the consent sought by the organization may vary, depending upon the circumstances and the type of information,[449] but without further specifying the appropriate said form.

The Wireless Consumers Alliance is of the opinion that such consent should be provided in a clear way[450] and that consent is not consent when hidden in an agreement or on web pages.[451] Furthermore MMA members are requested to obtain the consent of the wireless user through indigenous technological mechanisms available for wireless media.[452]

Also and with regards to this issue, the analysts' opinion is to the effect that it would be impractical to put pages of privacy disclosure information on a four-line wireless phone screen for a wireless user to click a button to opt-in or -out.[453] CTIA seems to be of the opinion that there are a myriad of ways by

---

446 Section 3, Article (b) (4) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); and Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages.

447 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages.

448 *Id.* and Section 3, Article (b) (4) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); and Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002).

449 Schedule 1, Section 5, Article 4.3.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

450 http://www.wireless-consumers.org/ (Last accessed on July 8, 2002)

451 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS CONSUMERS ALLIANCE INC., Comment (April 6, 2001), 8 pages, p. 2.

452 *Id.* WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 4.

453 Matt Hamblen, *Ensuring portable privacy - Banks, retailers and airlines face the 'opt-in' issue and other challenges*, COMPUTERWORLD,

which a LBS Provider may satisfy this consent requirement, such as signed service agreements, website subscriptions, *clickwrap* agreements, and user signaling via a handset or PDA.[454]

For this reason, there is not a unanimous decision regarding the form of the consent, and no one has taken into account the specific aspects of this type of service and the wireless device as well as the type of relationship the wireless user already has with his carrier.

3.2.3.1 Push and Pull

Wireless data is generally accessible in two formats, *pull data* or *push data*. *Pull data* involves the process of actively seeking and requesting wireless data using a wireless device and this process is similar to browsing for information on the wired web.[455] More specifically, the *pull advertising* model serves the consumer by promoting free content and involves placing advertisements on browsed wireless content. In this scenario, viewers surfing the wireless web will see ads when retrieving content from different websites.[456]

In this type of model, since it is the wireless user that initiates the dialogue or makes a request, the permission question becomes less critical and so do the privacy issues surrounding it. As a matter of fact, consent may be implicit in a transaction such as when a wireless user calls a location-based concierge service seeking driving directions to a specific restaurant. Also, in pull services, the location data information seems ephemeral and useful only to complete a requested transaction.

For example, and as the AAA[457] asserts, wireless users who use their location-based assistance service have very definite expectations that the AAA will use their location information to provide the service to which they subscribe.[458] In some cases, the consent can be implied by a person's specific actions as

---

December 11, 2000. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO54794,00.html (Last accessed on July 8, 2002)

454 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 9-10.

455 Windwire Inc., *First-to-Wireless: Capabilities and Benefits of Wireless Marketing and Advertising Based on the First National Mobile Marketing Trial*, December 27, 2000, p. 2.

456 *Id.* p. 4.

457 http://www.aaafoundation.org/home/ (Last accessed on July 8, 2002)

458 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and

stated in CTIA's Petition, especially in emergency situations.[459] On this last issue, Texas 9-1-1 Agencies[460] outlines[461] that it is of the general opinion that the caller, by dialing 911, implies consent to the disclosure of his location data.[462]

According to author Albert Gidari, there should be no requirement, for example, for the LBS Provider to obtain and record the wireless user's location used in providing the service, if such service was requested in the pull manner by the user.[463] However, when location data is stored and used to develop a wireless user profile, greater privacy concerns are implicated and in such case, even pull services can present disclosure issues.

Push data is information sent to devices as short bursts of text, generally 160 characters or less, sometimes called alerts or SMS. In the case of wireless advertising, *push advertising* involves pushing advertising messages to consumers, usually in the form of an SMS.[464] Privacy and consumer rights issues surround push advertising, since it is the model that is most likely to be intrusive considering it may be unsolicited.[465] For this reason, the present paper further analyzes the privacy issues based on push location-based services and advertising. As a matter of fact, permission is a necessity when you are talking about pushing messages to people. For example, when a retail chain broadcasts notices of sales to wireless users close to the geographic locations of their stores they need to know, with a high degree of certainty, whether the wireless user recipients are interested in receiving such information.

Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, AMERICAN AUTOMOBILE ASSOCIATION, Reply to Comments (April 24, 2001), 9 pages, p. 4.

459 *Id.* EPIC, Reply to Comments (April 24, 2001), 18 pages, p. 8.

460 http://www.nena9-1-1.org/texas/TX911Entities.htm (Last accessed on July 8, 2002)

461 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, THE TEXAS 9-1-1 AGENCIES, Comment (April 6, 2001), 5 pages, p. 3.

462 *Id.* CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 3 and Memorandum Opinion for John C. Keeney, Acting Assistant Attorney General, Criminal Division, from Richard L. Shiffrin, Deputy Assistant Attorney General, Office of Legal Counsel, U.S., Department of Justice, (September 10, 1996) (filed for CC Docket No. 94-102).

463 Albert Gidari, *Location Privacy: Fair Location Information Practices for Mobile Commerce*, Prepared for Location Decisions 2000 – Application of Location Technology for the International Commercial Environment, Chicago, Illinois, June 13-14, 2000.

464 Windwire Inc., *First-to-Wireless: Capabilities and Benefits of Wireless Marketing and Advertising Based on the First National Mobile Marketing Trial*, December 27, 2000, p. 4.

465 Rosalie Nelson, *Mobile Advertising: building alternative revenue streams*, OVUM, Short Report 20, June 2000, p. 7.

3.2.3.2 Opt in versus Opt out

The opt-in procedure of wireless companies is in stark contrast to the opt-out position of banks in the United States, which recently released a flood of mailings, which their customers had to return to avoid their personal data being used to market products and services. Analysts are of the opinion that the logistics of how consumers will opt-in and -out are not well defined and are raising several concerns.[466]

The two main issues include the tracking and the receiving of location-based services. It needs to be determined if the wireless user should be able to opt-in or opt-out of such tracking and the receiving of location-based services.

On the Internet side, the United States seem to be promoting an opt-out approach by most e-commerce websites now whereas Europe[467] and perhaps even Canada favors more of an opt-in approach. As a matter of fact, PIPEDA does suggest that the form of the consent may vary, depending upon the circumstances and the type of information.[468] It also suggests that in determining the form of consent to use, organizations shall take into account the sensitivity of the information.[469] At the same time, a recent release from the Privacy Commissioner of Canada seems to imply that opt-in is a much better way of gathering a user's consent:[470]

> I should begin by making it clear that, like most other privacy advocates, I have a very low opinion of opt-out consent, which I consider to be a weak form of consent reflecting at best a mere token observance of what is perhaps the most fundamental principle of privacy protection. Opt-out consent is in effect the presumption of consent – the individual is presumed to give consent unless he or she takes action to negate it. I share the view that such presumption tends to put the responsibility on the wrong party. I am also of

---

466 Matt Hamblen, *Ensuring portable privacy - Banks, retailers and airlines face the 'opt-in' issue and other challenges*, COMPUTERWORLD, December 11, 2000. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO54794,00.html (Last accessed on December 11, 2000)

467 European Commission, *Commission welcomes European Parliament's vote to accept directive on data protection rules for electronic communications sector*, Press release, IP/02/783, Brussels, May 30, 2002.
http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/02/783|0|RAPID&lg=EN (Last accessed on July 8, 2002)

468 Schedule 1, Section 5, Article 4.3.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

469 *Id.*

470 Privacy Commissionner of Canada, *Findings regarding complaints about Air Canada's Aeroplan Frequent Flyer Program under the Personal Information Protection and Electronic Documents Act*, New release, Ottawa, March 20, 2002.
http://www.privcom.gc.ca/media/nr-c/02_05_b_020320_e.asp (Last accessed July 8, 2002)

> the view that inviting people to opt-in to a thing, as opposed to putting them into the position of having to opt-out of it or suffer the consequences, is simply a matter of basic human decency.[471]

The privacy context may be different in the wireless world, since it involves the aspect of location and the fact that a wireless device is usually used by a single user, making this media more intrusive than on the Internet. In the context of location-based advertising, Evan Hendricks from Privacy Times,[472] raised the issue of opt-in versus opt-out:

> We heard (..) Mark talked earlier, he sees these services working only if they're opt-in, obviously if they're wireless data form, I heard Verizon and AT&T saying they need to be opt-in, CTIA says they ought to be opt-in, WAA they have to be opt-in. Does DMA take a stand on this? You have always been praying at the altar of opt-out for all these years, and I wondered if that will continue to be the same or if you see the advent of the 21st Century.[473]

Jerry Cerasale, Senior VP for government affairs at the Direct Marketing Association[474] (hereinafter the **DMA**), informed the FTC that DMA seems to be changing its views on this issue based on who pays for the location-based advertising. He answered that if the wireless user has to pay, it is clearly an opt-in type model but, if the customer does not have to pay, there should be a disclosure followed by an opt-out type model.[475] This type of reasoning may imply that, in the context of location-based services or advertising, LBS Providers could track a wireless user without their consent and could start sending advertising messages if such user is not paying for the SMS message. This sounds very intrusive.

Whether we are referring to the collection of location data or to the sending of unsolicited wireless messages, certain laws further detailed under Subsection 2.2 or industry players promote an opt-out

---

471 *Id.*

472 http://www.privacytimes.com/ (Last accessed July 8, 2002)

473 Evan Hendricks from Privacy Times, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 11, 2000, p. 38. http://www.ftc.gov/bcp/workshops/wireless/001211.htm (Last accessed July 8, 2002)

474 The Direct Marketing Association (The DMA) is the oldest (since 1917) trade association for users and suppliers in the direct, database and interactive marketing field. http://www.the-dma.org/ (Last accessed July 8, 2002)

475 Jerry Cerasale, Senior VP for government affairs at the Direct Marketing Association, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 11, 2000, p. 38. http://www.ftc.gov/bcp/workshops/wireless/001211.htm (Last accessed July 8, 2002)

procedure as a minimum requirement,[476] while others promote an opt-in procedure[477] or even a confirmed opt-in procedure.[478]

3.2.4 When Should the Consent be Obtained?

With regards to the time of the consent, we face the same controversy already discussed under Subsection 3.1.4. related to the time that the disclosure should be given. It must be determined if the consent should take place prior to the collection of the data,[479] prior to processing,[480] or even prior to using the collected data.[481]

It has been noted that the *U.S. Communications Act*[482] does not require consent prior to collection of location data, but requires that consent be given before the use or the disclosure of such data.[483] This

---

476 Article 2, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article 7 (2), Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1, European Union (2000); Section 5, (a) (5), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act, S. 630, 107th Congress, 21st Session (2001); Section 2 (a) (2), The Netizens Protection Act, H.R. 3146, 107th Congress, 1st Session (2001); and Section 5 (a) (3), The Unsolicited Commercial Electronic Mail Act, H.R. 95, 107th Congress, 1st Session (2001).

477 European Coalition Against Unsolicited Commercial Email http://www.cauce.com (Last accessed July 8, 2002); Section 2 (5); Section 3 (a) (1) (e), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Article 12, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

478 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002)

479 Article (2), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Section 3, Article (b) (1) (B) (i), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Schedule 1, Section 5, Article 4.3, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); and Article 43, Act to Establish a Legal Framework for Information Technology, Bill 161, 36th legislature, 2nd session, c. 32 (2001) (Quebec, Canada).

480 Article 7 a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Articles 6 (3) and 9 (1) Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

481 Article 2, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article 8, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada); and Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002)

482 The Telecommunications 4 Act § 7 U.S.C. § 222 Privacy of customer information (1996).

483 *Id.* § 47 U.S.C. § 222 (c) (i).

would imply that a LBS Provider may be entitled to track a wireless user and only obtain his consent prior to using the stored location data it has collected about such user, which seems also to be very intrusive in nature. Also, it is interesting to note that CTIA also promotes that the consent be made manifest and express prior to the use of location data.[484]

3.2.5 How Long Should the Consent be Valid for?

On this issue, the Electronic Privacy Information Center[485] (hereinafter **EPIC**), which a non-profit research and educational organization that examines the privacy and civil liberties implications of emerging technologies, suggested that a carrier should keep a record of consent for as long as the permission is valid.[486]

It is still to be determined how long the consent does or should last. For example, should it last only long enough to conduct a location-related transaction, or months, or years? It has been suggested that companies should focus on services where users provide explicit consent to process location data for each individual transaction.[487] This suggestion may be very impractical, especially for a LBS Provider looking to provide users with personalized and push location-based services.

As a matter of fact, in the case where the LBS Provider is collecting and storing location data in passive mode in order to process this information and provide wireless users with personalized content, it does not make sense for the consent to only be valid for one specific transaction. This would, therefore, make it impossible for content providers to make inferences on the interests and lifestyle of the wireless user,[488] since such inferences, in order to be accurate, must be based on collected location data over a long period of time.

---

484 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 10.

485 EPIC has brought lawsuits to accomplish privacy-protection goals that are rarely recognized in the federal and state legislative arenas. http://www.epic.org/ (Last accessed on July 8, 2002)

486 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, EPIC, Reply to Comments (April 24, 2001), 18 pages, p. 9.

487 See Research Note, *E-11-0929 Yahoo! Find-a-Friend: Wireless or Borderless Privacy?* From Andrea Di Maio, *New European Privacy Directive Addresses Location Data from Mobile Phones*, GARTNER INC., July 14, 2000.

A solution to avoid this may be to request that the wireless user specifies how long his consent is valid.

3.2.6 What Should be the Content of the Consent?

The first part of the consent that may be required from the wireless user is related to the tracking of his historical movement over time. Perhaps this type of consent should only be provided after the wireless user has obtained an explicit and detailed disclosure regarding the security and storage issues relating to his historical location data that will be collected.

Internet users have for years been complaining about unwanted email, or spam, with messages that promise everything from quick cash to an enhanced love life and consumers are now concerned about spam sent to their wireless devices.[489] For this reason, the second issue where the consent may be required from the wireless user is related to the actual receiving of the location-based services. For example, wireless users may opt-in to receiving messages but end up being bombarded with information from all stores as they are walking into a mall as was suggested by Matt Hamblen, from Computerworld.[490]

The legal framework related to the consent is to the effect that the wireless users should provide their consent on the collection of the data,[491] the use of the data,[492] and the disclosure or transfer of the data

---

488 In order to provide wireless personalization as further discussed under Subsection 1.3.2.

489 Patrick Ross, *Bill aims to block wireless junk email*, CNET NEWS.COM, January 10, 2001. http://news.cnet.com/news/0-1004-200-4432707.html (Last accessed on January 10, 2001)

490 Matt Hamblen, *Ensuring portable privacy - Banks, retailers and airlines face the 'opt-in' issue and other challenges*, COMPUTERWORLD, December 11, 2000. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO54794,00.html (Last accessed on December 11, 2000)

491 Article 7, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 2, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article (2), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Section 3, Article (b) (1) (B) (i), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Articles 5 (3) and 7, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002); and Article 43, Act to Establish a Legal Framework for Information Technology, Bill 161, 36th legislature, 2nd session, c. 32 (2001) (Quebec, Canada).

492 Articles 7 and 9, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Articles 6 (3) and 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a*

to third parties.[493] The wireless users shall also have the right to object, free of charge, to the processing of the data for the purposes of direct marketing[494] and to receiving unsolicited communications for direct marketing purposes.[495] Furthermore, the framework provides that the consent be obtained on the retaining[496] and storage[497] of the location data, and that the wireless user specifies the time for which the consent is valid.[498]

Research and consulting firm Ovum[499] suggested that companies offering location-based advertising should give the wireless user a strong element of control over the type, frequency and timing of advertisement delivery.[500] The legal framework never specifies that in the context of location-based services, the user should also provide consent regarding related issues, such as how many messages it wants to receive a day, from whom, and where and when it wants to receive these messages, etc.

Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, 15396/2/01, Brussels (January 29, 2002); Article 2, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article (2), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Section 3, Article (b) (1) (B) (i), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Article 5 (3), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Article 8, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada); Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

493 Articles 7 and 9, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Section 3, Article (b) (1) (B) (i), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); and Article 5 (3), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

494 Article 14 b), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Articles 11 1) and 12 1), Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997); and Article 9 (2), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

495 Article 13, Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

496 Section 3, Article (b) (1) (B) (i), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

497 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

498 Article 8, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

499 http://www.ovum.com/ (Last accessed on July 8, 2002)

500 Rosalie Nelson, *Mobile Advertising: building alternative revenue streams*, OVUM, Short Report 20, June 2000.

3.3 Data Quality

The legal framework related to the quality of the data provides that personal data is relevant to the purposes for which they are to be used[501] and, to the extent necessary for those purposes, should be accurate,[502] complete,[503] and kept up to date.[504] It also promotes that every reasonable step must be taken to ensure that data, which is inaccurate or incomplete, is erased or rectified[505] and that the data be kept in a form that permits identification of data subjects[506] and be obtained from a reliable source.[507]

The laws never specify if location data is considered quality data or what type of tracking technology should be used to ensure that historical location data or real-time location data is quality data. Also, the laws, while mentioning that every reasonable step must be taken to ensure that data that are inaccurate or incomplete are erased or rectified, do not specify what type of system should be developed by the LBS Provider to enable wireless users to update their profile data. Such system should comply with the legal framework and ensure that the collected data is quality data and that such data may easily be updated.

---

501 Article 8, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 6 c), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Article 5, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

502 *Id.* and Schedule 1, Section 5, Article 4.6, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Article 11, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada); Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

503 Article 8, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 5, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Schedule 1, Section 5, Article 4.6, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); and Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002)

504 *Id.* and Article 6 d), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Article 11, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

505 Article 6 d), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

506 *Id.* Article 6 e).

507 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last

3.3.1 Is Location Data "Quality" Data?

Location data can be used for personalization purposes, either by Dynamic Profiling through the use of historical location data or through the use of real-time location data. This may enable a content provider to send a message to a wireless user at the right place and the right time to make this message relevant, as previously explained under Subsections 1.3.2 and 1.3.3. It must be determined that the location data that is collected from the network-based or handset-based tracking technologies is obtained from reliable sources.

On the Internet, marketers like Doubleclick[508] have sought to personalize promotions and advertisements. Personalization is, potentially, a fantastic idea since one could customize offerings or content based on the tastes of each wireless user rather than having the same product or service for everyone.

Most arguments against personalization have come from the privacy angle, more specifically from consumers' concern for the data being collected about them. Also, many personalization systems are bound to irritate because of their presumption of knowledge about the user. For example, on the Internet when a user visits Amazon.com[509] he is greeted with a welcome back message and a *recommends* engine where, as soon as he chooses a book, he is provided with information about other books which may be of interest. Regardless, many personalization systems seek to summarize a human being by a string of numbers and, according to these systems, a human being can be defined by variables relating to past behavior and individual characteristics such as demographics.

This personalization process works differently on the wireless side. There could be an issue where we consider that the content provider that wants to have access to location data from the wireless users in order to make inferences about them and to send them personalized location-based services could be mistaken and make untrue inferences about the users. For example, a content provider looking to deliver a message to hockey fans may assume that a certain wireless user, that has been on the site of

---

accessed on July 8, 2002)

508 DoubleClick is a provider of broad range of technology, media, direct marketing, email, and research solutions. http://www.doubleclick.com/ (Last accessed on July 8, 2002)

a stadium on many occasions at a specific time during which a hockey game was taking place (use of historical location data) is a hockey fan. The truth may be that such wireless user is simply an employee of the stadium. The same analogy could be made where the content provider assumes that a wireless user visiting a stadium on a Saturday night (real-time location data) may be interested in receiving a coupon for a beer, without taking into account that such user may be an employee of the concession company.

Also, individuals are not always necessarily defined by their past behavior. No single choice defines them nor does it satisfactorily predict their future behavior. For this reason, and since human inferences will be made based on the collection of location data over a period of time (or historical location data), it is yet to be determined if location data can be considered as quality data. It is also to be determined if personalization may be a flawed approach of the wireless space, where we may need to ask ourselves if it is possible to identify a set of behavioral/demographic variables that collectively describe the essence of a human being.

One should also evaluate the quality of the location data being collected and used in connection with the type of tracking technology that is being used to collect this data, since quality may also imply accuracy of the collected location data.

3.3.2 What Type of Tracking Technology Should be Used?

It is interesting to note that certain authors are of the opinion that location-based services will never be successful because of issues related to the accuracy of location tracking technologies.[510]

An analysis of the different types of location tracking technologies may be made in order to address the quality of the location data and help determine what is the appropriate type of location tracking technology. Such tracking technology should be used to ensure that the collected location data is accurate and, therefore, of quality.

---

509 http://www.amazon.com/ (Last accessed on July 8, 2002)

510 Mike Banahan, *Location Aware Services – Beware*, July 2000. http://www.gbdirect.co.uk/ouropinions/locationaware.htm (Last accessed on July 8, 2002)

Each of the tracking technologies, namely the network-based technology and the handset-based technology, has its benefits and its disadvantages.

3.3.2.1 Network-based Location Technology

The major advantage of using a network-based location determination technology is that the system works with all existing handsets and networks[511] since the communication of a mobile device to a fixed base station or cell tower is inherent to any wireless communications system. Any wireless device that is *powered-on* needs to periodically register with the nearest base station in order for calls to be routed to that device.

The collection of these periodic registrations and other wireless network events allows for the passive tracking of the device location in a continuous fashion. The location data obtained in passive mode, also known as historical location data, can be archived or used to build sophisticated customer profiles as previously mentioned under Subsection 1.3.2.

Problems with this type of technology include the fact that they suffer from poor accuracy.[512] As a matter of fact, Cell ID technology has wide variations in the precision of the location data,[513] where in a typical city area a cell size may be approximately 150 meters contrasted with a typical rural area where a cell size may be 2 km or more.[514] More precise location data, according to Forrester Research, may be obtained with solutions that measure not only the distance between phones and base stations but also proximity to fixed objects or orbiting satellites, such as GPS.[515]

Also, to enhance the accuracy of the location data, operators can deploy software-based solutions based either in the network (also known as network-enhanced Cell ID technology) or in the handset. This last solution calculates the time needed for signals from multiple base stations to reach a phone, enhancing the Cell ID accuracy up to fifty percent (50%)[516] especially in rural areas.[517]

---

511 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, p. 3.

512 *Id.*

513 *Id.* p. 4.

514 *Id.*

515 *Id.* p.3.

516 *Id.*

3.3.2.2 Handset-based Location Technology

The most common handset-based location determination technology is GPS that benefits from extremely high accuracy (it has a 1 meter precision radius).[518] Furthermore, an important distinction between network-based and GPS technology is that GPS can provide altitude and vector. Network-based location determination technology does not have that capability as of today, but this may change in the future. Altitude and vector are important if the LBS Provider is not tracking the person and uses single instance of location for queries. GPS determination would allow the LBS Provider to determine if there is a traffic jam ahead, since the technology would know the direction and speed of the user. Altitude would also allow the LBS Provider to give the user very detailed location data; for example, on which floor of the mall the bathroom is located and how to get there. Altitude provides the addition of the z-axis to location determination technology, which is typically limited to x and y coordinates.

For this reason, GPS provides more accurate information and so better data quality, especially if there is a real-time trigger. Furthermore, GPS chips, have shrunk to the size of postage stamps, which could make it that much easier to build precise location sensors into phones and other devices.[519]

SiRF Technology[520] pointed out that the present location technology used today is not very accurate[521] but that this would be different with GPS technology:

> This problem is significantly reduced when a GPS phone automatically transmits a roadside location with a 15 meters radius. It would be enormously increased by calls coming from a handset that reported a 750-meter radius, which would include a mile-long stretch of the freeway.[522]

---

517 *Id.* p.4.

518 *Id.*

519 Matt Hamblen and Bob Brewin, *Need to Find A Customer?*, COMPUTERWORLD, April 16, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59621,00.html (Last accessed on July 8, 2002)

520 SiRF Technology Inc. is a leader in GPS Enabled Location Technologies. http://www.sirf.com/ (Last accessed on July 8, 2002)

521 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SIRF TECHNOLOGY INC., Notice (April 30, 2001), 14 pages, p. 5-7.

At the same time SiRF[523] has raised the downside of the accuracy that may wrongly place a wireless user at the scene of a crime.[524] Also, the GPS receiver chip would have to fight for scarce space on handsets that are already crowded with voice-recognition and Internet access functions. Generic GPS also has problems related to speed and finding open space indoors[525] and in congested urban areas, all driven by the inherent requirement for a line of sight for all satellites-based technologies. Solutions for this include enhanced GPS, like that from Snaptrack,[526] where servers refine and improve the GPS data based on historical and predicted future locations.

A major inhibitor of GPS for constant location determination (or tracking) is the large power requirements of GPS receivers. Constantly calculating a device's location based on the raw satellite data consumes a relatively large amount of battery life in any given handset, thereby reducing the available functional time of the handset for its primary purpose, which is communication. This may change in the future with the advent of improved battery technologies and enhanced power conservation of GPS receivers but this is a very real issue today.

A downside of this type of technology is that the constant calculation of a GPS-based location upon user activation in the handset necessarily precludes passive tracking. A LBS Providers' GPS location tracking technology cannot track and store a wireless user's location and movements over time. For this reason, such technology cannot realistically be used for tracking since, to get the location information to a content provider, one would have to figure out a way to get it out of the phone, which is not trivial and consumes precious network resources.

Therefore, the LBS Provider using this type of technology will not be in a position to use historical location patterns of the wireless users in order to provide these users with personalized predictive services. This may diminish the quality of the location data.

---

522 *Id.* p. 7.

523 http://www.sirf.com/ (Last accessed on July 8, 2002)

524 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SIRF TECHNOLOGY INC., Notice (April 30, 2001), 14 pages, p. 7.

525 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, p. 4.

526 http://www.snaptrack.com/ (Last accessed on July 8, 2002)

3.3.3 What System Should be Used to Ensure the Data is Quality Data?

The type of system to ensure that location data is quality data may include a function of the system that would enable the cross-aggregation of data. On the other side, other privacy issues would be related to such new system that may involve personal data, similar to the ones we have seen on the Internet. This issue was raised by Martin Reynolds, in an article entitled: *Wireless Location Services: Who's Watching You?:*

> One challenge to privacy in the Internet age is that of cross-aggregation. For example, magazine subscription lists are available for a relatively low fee. These lists could be cross-correlated to provide the magazine subscription profile of any individual as part of a database and provided to interested parties without the knowledge of the individual concerned. Would, for example, a school look unfavorably on a prospective teacher with a subscription to "Guns and Ammo" or "Playboy?" Computer technology provides the ability for cross-aggregation of all such cross-tabulated data. Internet tracking companies, such as DoubleClick, have threatened to perform massive cross-aggregation in the past but have publicly backed down because of privacy concerns. However, it is likely that cross-aggregation will grow as a source of semiprivate information about consumers; the Internet enables this intrusion to happen offshore, out of the reach of government privacy initiatives. Cross-aggregation is one of the great threats that computer systems pose to individual privacy.[527]

Perhaps the appropriate technology system could ensure that the wireless user that has agreed to receive location-based messages also be involved in the creation of his profile on a voluntary basis. Also, a technical system anonymizing and managing this personal data may be part of the solution. As a matter of fact, the legal framework to the effect that the collected data be kept in a form that permits identification of data subjects[528] is not relevant in the context of providing location-based services, where anonymization may benefit wireless users, as further detailed under Subsections 3.4.3.1 and 4.4.3.1.

---

527 Martin Reynolds, *Wireless Location Services: Who's watching You?*, GARTNER INC., May 9, 2001. http://www3.gartner.com/DisplayDocument?id=329970&acsFlg=accessBought (Last accessed on July 8, 2002)

528 Article 6 e), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

3.3.4 What System Should be Used for Updates?

How can wireless users be able to correct inaccuracies in their profile data if we are talking about location data and the fact that inferences will be made by third party content providers using this type of data? As a matter of fact, a user would not be able to predict what will be the inferences made by the content providers wishing to push messages to him based on a profile inferred by his actual location (real-time location data) and his past behavioral patterns (historical location data). For this reason, how will it be possible for such user to update and correct any inaccuracies in his profile?

Also, in some cases, a LBS Provider may be interested in using anonymous location data and creating some type of system where the parties involved in providing the location-based service do not know the identity of the user. For example, the identity of the wireless user would not be known either by the party actually storing the historical location data or by the content provider looking to have access to location data, to create a profile, or to plan a marketing campaign. In that event, how would it be possible for a wireless user to refer to his profile and correct inaccuracies given that his identity has been removed?

3.4 Data Security

Certain authors seem to imply that privacy policies may not be enough when it comes to protecting the privacy of wireless users. Forrester Research,[529] in one of its reports regarding wireless privacy, outlines the fact that service providers will need to do more than adopt a privacy policy in order to protect wireless users:

> Attendees wrestled with the problem of how a company can provide a proper privacy notice on a WAP screen that's only four lines long. But the lack of screen place isn't the real issue – it's the lack of space in the consumer's day to become a lawyer, grind through privacy contracts at every turn, and drive the market toward good policies. Companies will need to do more to fundamentally reform their information practices, rather than trying to put lipstick on a pig by merely posting a privacy policy.[530]

---

529 http://www.forrester.com/ (Last accessed on July 8, 2002)

A suggestion may well be to implement technical security measures in order to protect the privacy of wireless users. Such technical security measures would have to be in line with the legal framework related to the security of the collected personal data, which requires that data be protected against accidental loss or theft, unauthorized disclosure or access, accidental or unlawful destruction, modification and alteration, unlawful processing, copying, and use or misuse.[531]

Furthermore, such framework mentions that the methods of protection should include reasonable security measures that involve organizational measures (for example, access on a need-to-know basis), technological measures (for example, the use of passwords and encryption), and physical measures (for example, locked cabinets and restricted access to offices).[532] Also, these security measures shall take into account the state of the art and cost of implementation, the method of storage, the nature and sensivity of the data, the amount of data collected and the distribution of such data.[533] PIPEDA further requires that organizations protect personal information regardless of the format in which it is held,[534] which seems to imply that location data should also be protected, regardless of its unusual format.

---

530 Jay Stanley, *Wireless Ushering In A New Phase In Privacy Wars*, THE FORRESTER BRIEF, December 21, 2000, p. 1.

531 Article 11, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 17 1), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Article 4, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Schedule 1, Section 5, Article 4.7.1, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

532 *Id.* and Article (3), The Wireless Privacy Protection Act , HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Section 3, Article (b) (1) (D). The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Schedule 1, Section 5, Articles 4.7 and 4.7.3, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Article 10, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada); and Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages.

533 Article 17 1), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Schedule 1, Section 5, Articless 4.7.1 and 4.7.2, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

534 Schedule 1, Section 5, Article 4.7.1, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

At the same time, the legal framework related to data security does not specify which tracking technology should be considered the most secure technology in order to safeguard the data and should, therefore, be used by a LBS Provider. Furthermore, the laws and regulations never specify what type of system would be adequate and considered *reasonable* or *appropriate*.[535]

Since the laws do not propose a specific solution and are in that way vague as to what may be considered appropriate or reasonable under the circumstances, a LBS Provider looking to deploy location-based services has to analyze the unique characteristics of this new type of service. Once analyzing the characteristics of this new media, the LBS Provider will have to come up with the appropriate technological system and/or business model to provide these types of services, while keeping the collected location data secure.

3.4.1 What is the Most Secure Tracking Technology?

Advocates of the handset-based technology system argue the fact that this technology would answer many privacy concerns. They are basing their reasoning on the fact that this technology allows wireless users to manually disable the ability to locate them, thereby avoiding surveillance.[536]

They further believe that a handset-only system may ensure greater privacy because the network is not constantly accumulating data. The users can also turn on and off their location transmission, therefore allowing the wireless user to control when his location is given out.[537] These authors also point out that this system would display the coordinates of the phone's location to the person carrying it, therefore providing a security tool for its users.[538] For example, a wireless phone user could call a friend after running out of gas and tell the potential rescuer where to find the car by reading his position off the phone's screen.

---

535 Article 17 1), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Schedule 1, Section 5, Article 4.7, 4.7.2, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

536 Joanna Glasner, *Feds OK Cell Phone Tracking*, WIRED NEWS, September 16, 1999.
http://www.wired.com/news/topstories/0,1287,21781,00.html (Last accessed on July 8, 2002)

537 Peter Wayner, *Technology that tracks cell phones draws fire*, N.Y. TIMES, February 23, 1998.
http://www.nytimes.com/library/tech/98/02/biztech/articles/022398track.html (Last accessed on July 8, 2002)

This is apparently a controversial issue, since others players like Sprint PCS[539] prefer the network-based solution, also for security reasons:

> But there is a real concern about where the location information will be transmitted from, and this was recently brought up at the WAP forum last week. I don't know if it was resolved. I doubt that it was resolved, but as we understood the proposition by certain handset manufacturers, the location information would be transmitted from the handset, and we are strongly opposed to that. We believe that the information should be transmitted from the network, and the business rules established in the network because our network is highly secure, it's protected by firewalls and all other types of security devices. A handset in contrast is at best a very simple computer, and it will be a lot harder to protect a handset from being hacked into by an unwanted third-party application than it will be, for our network, to be hacked into.[540]

There appears to be both pros and cons relating to the security of the data for both technologies. Perhaps in determining the most secure technology, we may want to take into account other factors including the fact that the tracking technology used may be secure in the event that location data is collected anonymously by being encrypted at the source. Also, we may want to evaluate the benefits of one technology over the other with regards to the quality of the collected data, as further detailed under Subsection 4.3.2.

3.4.2 Who Should Handle the Sensitive Data?

The LBS Provider, prior to adopting an appropriate business model, has to ensure that the sensitive information collected will be in the custody of a trusted third party, perhaps even in the custody of the wireless user himself.

3.4.2.1 Should it be the Wireless User?

Many authors suggest that the profile of the wireless user including his personal information be kept within the custody of the user, and so in his device. This solution has also been proposed by Gregory

---

538 *Id.*

539 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

540 Joseph Assenzo, Sprint, participant at the Federal Trade Commission – Panel on location-based services and advertising: possibilities and privacy concerns, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues,*

Miller, VP of Corporate Development and CPO of Meconomy,[541] on a Panel on building privacy and security solutions into the technological architecture:

> First the user's direct access device should be the initial source of encryption. We believe it should be performed end to end without untrusted intermediaries. Secondly, we think the end device should be an open platform so users can load and unload their own privacy and security technologies. (...) And finally any data collected for a transaction should be decoupled from personally identifiable data and only used for that transaction.[542]

The same author, it his article entitled: *Building Privacy and Security Solutions into the Technological Architecture*, says that it may not be very practical to have the profiles in the hands of the user and that it may be a good solution to focus on leveraging trusted relationships:[543]

> Centralization is a difficult proposition to resist, but peer-to-peer technology may be the natural antidote. Distributing data with strong crypto protection may afford a competent, feasible, and consumer comforting solution. Consider how gateway providers and intermediaries might maintain the aggregate data they want and need to render their services, but allow the actual profiles to remain directly in the control of their rightful owners - the consumer. On the other hand, in some settings, this may prove less than practical. Accordingly, we believe it comes down to having a strong trust relationship. If a trust relationship exists, then the aggregation of data into centralized databases may not be a pressing matter.[544]

The problem with this type of solution is that if the device was to store simultaneously the location and the profile, the LBS Provider will not be able to passively track the wireless users in order to Dynamic Profile them using historical location data in accordance with Subsection 1.3.2.[545] As a

---

Wireless Web Workshop, December 12, 2000, p. 36. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

541 MEconomy is committed to delivering solutions to the enterprise and to security technology providers that enhance trust and enable consumer and employee protection. http://www.meconomy.com/ (Last accessed on July 8, 2002)

542 Gregory Miller, VP of Corporate development and CPO, MEconomy, participant at the Federal Trade Commission – Panel on building privacy and security solutions into the technological architecture, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 44.
http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

543 Miller, Gregory A., *In re The Mobile Wireless Web, Data services and beyond: Emerging technology and consumer issues, A Public Workshop – Response Statement for Day II panel: Building Privacy and Security Solutions into the Technological Architecture*, December 11, 2000. http://www.ftc.gov/workshops/wireless/comments/miller.htm (Last accessed on July 30, 2001)

544 *Id.*

545 Mike Chartier, Intel, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000.
http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

matter of fact, an ideal system would protect the privacy of wireless users while allowing them to benefit from this type of dynamic personalization.

At the same time, the wireless user should be involved in the management of his profile, probably not through the device itself (since the screen of the wireless device is too small to do so) but through a Profile Manager mechanism, as further discussed under Subsection 4.3.3. According to the Static Profile function of the Profile Manager system, the user should be able to say, "you can only track me when I am downtown" (location) or "during the day" (time), therefore ensuring that his requests are always respected when his location data is collected and used for profiling purposes.

Finally, we also have to keep in mind that, regardless of the type of tracking technology that is being used, wireless users can always shut down their phone to disable the tracking.

3.4.2.2 Should it be a Third Trusted Party?

The appropriate solution may not provide for the wireless user to completely manage his location data and profile information for practical reasons further explained under Subsection 3.4.2.1. For this reason, we need to determine who should be the third party managing and handling the sensitive location data or involved in the hosting of the databases of profiles and historical location data. Should it be the carrier that already has a trusted relationship with the wireless user? the LBS Provider? or the content provider?

3.4.2.3 Should it be the Carrier?

Carriers can in a general way only use their subscriber's location data for telecommunications service purposes, such as ensuring quality of service and maintenance of their infrastructures, billing schedules, and churn management. In other words, carriers cannot, in certain and most markets, use this information for marketing and other purposes that go beyond telecommunications services, simply because national laws prevent them from doing so.

For example, in the United States and in Canada, federal law protects wireless phone users' location data from being given away by carriers without their consent, as further detailed under Subsection 2.5.

In the U.S., the *Wireless Communications and Public Safety Act* permits release of location data in emergencies for wireless telephones specifically, but the FCC's definition of what constitutes a phone is still legally unclear, says David Sobel, General Counsel for the EPIC.[546]

Relating to this issue, CDT outlines the fact that carriers have a duty to protect the confidentiality of customer information, which includes location data:

> To the extent a third party obtains location information relayed through a traditional CMRS carrier's facilities, such information would clearly be covered by the statute. Section 222 does not merely prescribe certain privacy rules that telecommunications carriers are bound to follow. It also generally charges them with "a duty to protect the confidentiality" of customer information (section 222 (a)).[547]

Evan Hendricks from Privacy Times[548] raises the fact that carriers may be in the best position to store the location data in order to avoid privacy issues since they are covered by privacy laws:

> It's the accumulation of personal details and the profiles that are dynamic that show where you're going, and that information can be stored by a third-party, and unless it's a carrier covered by the law described by the FCC official, that might not be protected by law, and then if you throw in advertising -- unwanted advertising on cell phones, you see that the whole wireless experience brings all the huge privacy concerns together, surveillance, SPAM, profiling and brings them together under one issue.[549]

James Schlichting from the FCC states that carriers will be, in most cases, legally bound to protect the personal information of their subscribers:

> Then the question of -- there is another provision related to emergencies of other subscriber information that can be released with regard -- released more specifically to emergency service providers, and this goes to the names, telephone numbers, addresses, and 222 (G) provides "The carrier shall release that information but only to the providers of emergency services for the use with regard to the provision of emergency services." So that's a very

---

546 http://www.epic.org/ (Last accessed on July 8, 2002)

547 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CENTER FOR DEMOCRACY AND TECHNOLOGY, Comment (April 24, 2001), 22 pages, p. 14.

548 http://www.privacytimes.com/ (Last accessed on July 8, 2002)

549 Evan Hendricks, Privacy Times, participant at the Federal Trade Commission – Panel on location-based services and advertising: possibilities and privacy concerns, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 35. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

> quick overview of a lot of information. What I have focused on and what the laws the FCC administers and what the FCC's regulations focus on is the privacy protections and wireless location information, the carriers, telecom carriers subject to the FCC jurisdiction have available to them and what they may or may not do. One of the questions that I think people need to worry about is when that information, location or otherwise, goes to folks that are not carriers, and it's not provided to the carriers' part of your subscription to a telecom service, these protections don't apply, but if you're talking about information that a carrier has by virtue of their relationship to you as a subscriber, these protections do apply.[550]

Finally, Ericsson[551] also outlines the problem that carriers would face if other parties handling location data would start spamming the carriers' subscribers:

> For example, a consumer would likely buy and use a location-based service from his wireless carrier. However, the location service itself may actually be provided by an overlay location provider. If the consumer begins to receive unsolicited communications, the consumer may believe that his/her principal carrier released private information.[552]

Carriers recognize today that they have a large amount of responsibility to manage data in a very effective manner with all the privacy issues that are inherent. Having said that, they also have a tremendous opportunity to monetize that data, and that is the issue.

These carriers have access to the location data of their subscribers in most cases and they also know the identity of the user (PII). For this reason, the privacy danger lies in the correlation of the user to the phone and the aggregated location data. This is why carriers are in a very delicate situation if they were to manage both the wireless user's PII (name and phone number) necessary for providing standard telecommunications services and the profile data (location data and Static Profile data).

---

550 James Schlichting, FCC, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues, Wireless Web Workshop*, December 12, 2000, p. 22. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

551 http://www.ericsson.com/ (Last accessed on July 8, 2002)

552 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, ERICSSON INC., Comment (April 6, 2001), 4 pages, p. 3.

3.4.3 What Type of Technology Security System should be Developed?

Certain authors are of the opinion that a Chief Privacy Officer and a security audit could provide the necessary conditions for ensuring location data security.[553] Others like Peter Swire, Chief Counselor for Privacy in the Office of Management and Budget, are of the opinion that this type of data would be more protected through security infrastructure:

> Whatever privacy practices develop generally for wireless information, I urge you to consider how to build an infrastructure that will also assure proper privacy protections for the most sensitive information.[554]

Lawrence Ponemon from Pricewaterhouse[555] suggests that LBS Providers should build the right security infrastructure in order to avoid the location data getting into the wrong hands.[556]

The security system should include physical measures,[557] organizational measures,[558] and technological measures.[559] Such system should also minimize the collection of sensitive data and ensure that the parties involved in the providing of location-based services only know what they actually need to know to provide their services. This would promote the security of the personal and location data of the wireless users.

3.4.3.1 Minimizing the Collection of Sensitive Data

Ideally, the LBS Provider system should minimize the collection of PII about the wireless users either when it is tracking them or when it is profiling them. As a matter of fact, a way to solve the privacy issues on the security side might be to minimize the collection and storage of PII. This may be done

---

553 Euro Beinat, *Privacy and Location-based Services: Stating the policy clearly*, GEO INFORMATICS, September 2001.

554 Peter Swire, Chief counselor for privacy in the Office of Management and Budget, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues, Wireless Web Workshop*, December 12, 2000, p. 2. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

555 http://www.pwcglobal.com/ (Last accessed on July 8, 2002)

556 Lawrence Ponemon, Pricewaterhouse, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 4. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

557 Schedule 1, Section 5, Article 4.7.3, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

558 *Id.*

559 *Id.*

through the adoption of the right business model and development of the appropriate technology system, as suggested by Lorrie Faith Cranor from AT&T Labs research:[560]

> But I think that there's a lot of things that companies that are doing marketing, they have all sorts of fancy algorithms that allow them to try to match you up to different sorts of things. I think they can also use that in order to reduce the amount of data that they have to keep on you so it serves their marketing purposes without having this complete dossier on you.[561]

The goal would be to remove the privacy threat to ensure that the data is secure. If the PII were to be removed from the databases storing the Static Profile data and location data, then wireless users would feel less threatened or worried that a third party might have access to their personal information and misuse it. Allan Davidson from the CDT also suggests this concept in order to solve the security issues:

> The base line answer is if you can find ways to deliver the services without keeping the information, you'll be doing yourself a huge favor and the consumer a huge favor.[562]

In some cases, the development of an appropriate technology system may solve privacy issues. The focus on technology such as firewalls or encryption has, in some cases, cast privacy as a technical matter rather than a policy one. On the other hand, one problem with anonymization is that encryption can be a heavy burden in the key management process, something worth considering when developing a security system, as pointed out by Gregory A. Miller:

> Encrypting data is a good measure, however, the challenging part, and the real focus ought to be verifying that the authorized individuals and only those authorized have the necessary keys. Assuming, however, that key management is properly maintained, encryption of data should be a business and/or utility proposition, predicated on the corresponding issues of ease of access, overhead, usability, performance, cost, etc. Simply encrypting all data will not solve the challenges of data protection, and in particular, the real issue is key management and security.[563]

---

560 http://www.research.att.com/ (Last accessed on July 8, 2002)

561 Lorrie Faith Cranor, AT&T Labs research, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 7. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

562 *Id.* Alan Davidson, attorney, CDT, p. 8.

563 Miller, Gregory A., *In re The Mobile Wireless Web, Data services and beyond: Emerging technology and consumer issues, A Public*

For this reason, a potential solution may be the designing of a network-based system that would anonymize the wireless users' PII, the location data and the Static Profile data at the carrier level, therefore minimizing the key management issues. Such system could include an identity proxy so that the LBS Provider only knows a pseudonym of the wireless user.

3.4.3.2 Separating the Knowledge of Each Party Involved

The second way of securing the location or personal data of the wireless users may be to separate the information given to each party involved in the providing of the location-based service, from the carrier, the LBS Provider and to the content provider (or advertiser). This type of solution would ensure that each party only knows what they actually need to know to provide the location-based service to the wireless user.

In order to put together a three-tier system where each party would only know part of the profile data, the LBS Provider should be different than the carrier. Such system would separate what the party in possession of the identity of the wireless users (the carrier) knows from what the party in possession of the Static Profile data and location data (the LBS Provider) knows.

At the same time, we have to keep in mind the crucial role of the carrier as further detailed under Subsection 4.1.2, which such security system should take into account.

3.4.4 Storage Related Issues

Information in databases is subject to a wide range of risks, requiring appropriate privacy and security measures. The risks include misuse by insiders,[564] unintentional or mistaken disclosure and/or access by unauthorized individuals. Also, because location data reveals the whereabouts of the individual

---

Workshop – Response Statement for Day II panel: Building Privacy and Security Solutions into the Technological Architecture, December 11, 2000. http://www.ftc.gov/workshops/wireless/comments/miller.htm (Last accessed on July 30, 2001)

564 A recent Information Security survey revealed that information theft by insiders in a company poses greater threats than external security branches. 24% of respondents reported electronic theft or sabotage or proprietary information; 58% reported abuse of employees computer access controls. Information Security, *Security Focused*, September 2000, p. 47.
http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf (Last accessed on July 8, 2002)

(often in real time), the potential for privacy intrusion and other problems is more serious than with other types of personal information. In extreme cases improper disclosure of location data could place a person in physical danger and could be misused by stalkers or in domestic disputes.

A database could also reveal when and where two or more users of wireless devices were in physical proximity. How will this proximity information be recorded and used?

For this reason, it is important to cover all the issues related to the databases, including where the data resides, who is hosting the databases, who has access to it, the length of time the location data is stored, and how securely stored is the data.

3.4.4.1 Where Should the Data Reside?

Should the data be stored on the carrier's side, on the LBS Provider's side, on the device itself, or on a server somewhere? This decision is crucial and we need to consider the fact that the carrier may be in a potential conflict of interest if it was to host the databases containing the location data and the Static Profile information. As a matter of fact, such conflict is based on the fact that the carrier already knows the identity of its subscribers, their names and phone numbers. For this reason, it may not be the best entity to also host the database containing location data (and/or Static Profile data) since it would now know far too much detailed information of the wireless users; namely, their identity, their profile information, and their every single location and movement through time.

3.4.4.2 Who Should Have Access to the Data?

The party hosting the database will necessarily have access to the location data and perhaps even the Static Profile information. Should the content provider that wants to access the Static Profile information and historical location data of the users, in order to target them with personalized push messages, also have access to this sensitive information?

Perhaps the real question is: Who needs to have access to the location data? The content provider needs to know if the wireless user it is targeting has the right profile to make the message relevant, but they may not need to know the identity of the user. As a matter of fact, content providers simply need

to know that these people have the appropriate profile for the message. The party actually sending the messages to the wireless user--perhaps this would be the carrier--needs to know the user's phone number but they do not need to have access to the location data or the Static Profile information of such users. For this reason, in the event that the carriers are delivering the messages to wireless users, they may not also need to have access to the database containing the user's location data and Static Profile information.

3.4.4.3 For How Long Should the Data be Stored?

The legal framework generally suggests that personal information be retained only as long as necessary for the fulfillment of the initial purposes. With regards to location data, the initial framework related to location data provided that location data be erased or made anonymous as soon as the communication ends and that it only be kept for the purpose of subscriber billing and interconnection payments.[565] Also, such location data could only be kept up to the end of the period during which the bill could lawfully be challenged or payment pursued.[566] Recently, such framework has been amended to confirm that the location data may be kept for the time necessary to accomplish the purposes of providing value-added services,[567] therefore taking into account the context of the new type of services, which are location-based.

PIPEDA further suggests that organizations should develop guidelines and implement procedures with respect to the retention of personal information, which guidelines should include minimum and maximum retention periods,[568] without specifying what should this period be and how to evaluate what would be an appropriate period.

Furthermore, with regards to the time that the historical location data would or should be stored, CDT, in its comments provided in the context of CTIA's Petition, observes that the privacy risks increase

---

565 Articles 6 (1) and 6 (2), Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

566 *Id.*

567 Article 6 (3), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

568 Schedule 1, Section 5, Article 4.5.2, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

when information is collected over protracted periods of time.[569]

To this effect, CTIA states that it assumed that location detail should be ephemeral and not stored.[570] SiRF[571] agrees with such comment:

> Old location information is less valuable to advertisers and commercial users and potentially more threatening to consumers. Location information should not be stored longer than necessary to bill (and resolve any disputes) unless it is part of a customization service about which the customer is periodically reminded in writing.[572]

SiRF[573] has also expressed the opinion that there ought to be limits for how long location detail is kept.[574] They further mention that unless the user affirmatively requests that information be stored to create an automatic profile to customize services, the location details should be destroyed within a few billing cycles.[575] This reasoning seems to be in line with the initial *EC Directive 97/66/EC* that provides that telecommunication traffic data must be erased or made anonymous as soon as the communication ends.[576]

Not only different countries may disagree on the period that should be appropriate for the storage of location data, but so do the players from the wireless space. As a matter of fact, in answer to SiRF's comment that entities must notify consumers if they retain information longer than *three billing cycles*, Sprint PCS[577] states the following:

---

569 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CENTER FOR DEMOCRACY & TECHNOLOGY, Comment (April 6, 2001), 13 pages, p. 5.

570 *Id.* CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 10.

571 http://www.sirf.com/ (Last accessed on July 8, 2002)

572 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SIRF TECHNOLOGY INC., Notice (April 30, 2001), 14 pages, p. 8.

573 http://www.sirf.com/ (Last accessed on July 8, 2002)

574 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SIRF TECHNOLOGY INC., Notice (30 April 2001), 14 pages, p. 9-10.

575 *Id.*

576 Article 6 (1), Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

577 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

> But there is no basis in the record for the Commission to determine that a three-month period, as opposed to a two- or four-month period (or some other period), is appropriate – or that any other rules on this subject are appropriate.[578]

Not only is Sprint's[579] opinion founded to the effect that SiRF's[580] comment is arbitrary, but this may also cause a potential problem with regards to the value of location-based services. As previously mentioned under Subsection 1.3.2, the collection and storage of historical location data would enable a LBS Provider to create Dynamic Profiles about wireless users. This would enable a LBS Provider to provide wireless users with very personalized and push location-based services based on such user's historical movements over time. This means that any system that would prohibit the storage of location data over time may not enable wireless users to benefit from this type of personalization.

There may be a system where the LBS Provider is able to use historical location data to provide personalized location-based services while also protecting the privacy of the wireless users. With regards to this issue, the law seems to be leaving the door open to simply anonymizing the location data instead of deleting it.

As a matter of fact, the *EC Directive 97/66/EC* also provides that telecommunications traffic data must be erased or made anonymous as soon as the communication ends,[581] leaving the door open for anonymization in the case of the collection of location data. The problem may be solved by requesting the wireless user's consent on this particular issue, as further discussed in Subsection 4.2.6.

Finally, the last issue deals with the Static Profile information that may also be stored. Should it have the same treatment and stored for the same period as location data?

---

578 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Reply to Comments (April 24, 2001), 16 pages, p.9.

579 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

580 http://www.sirf.com/ (Last accessed on July 8, 2002)

581 Article 6 (1), Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

3.4.4.4 How Secure Should the Storage be?

In order to determine how secure the storage should be, it is important to understand what kind of sensitive information would be stored in the databases. These databases may contain the historical location data of the wireless users as well as their Static Profile information. It is to be determined if they will also contain the users' names and/or phone numbers. In other words, a system may not have to be as secure if it is storing anonymous data, since a breach--or third party access to it--may not be as threatening to the individual to whom it belongs, given that it would not be identifiable to that person.

As a matter of fact, the PII of the wireless user may be anonymized for storage in these databases to make them more secure in the event of a breach or unauthorized third party access. If this is the case, then the security of the databases will most likely not have to be as strong as it would have to be if the databases contained PII. Still, in the event that PII is anonymized, we need to further discuss the technical solution that would be used. How would it be done? If it is through encryption, what type and strength of encryption should be used? How many keys would there be and who would be holding the key(s)?

3.5 Data Transfer

The legal framework related to the transfer of personal data prescribes that individuals be given the opportunity to choose and provide their unambiguous consent on whether, and the manner in which, a third party uses the personal information they provide.[582] This rule further applies when such use is

---

582 Article 26 (a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Article 3, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article (1) (C), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Section 3, Article (b) (3), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); The Telecommunications Act § 47 U.S.C. § 222 Privacy of customer information (1996); The Communications Act § 47 U.S.C. § 222 Privacy of customer information (1934); Article 13, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada); Section 7, Telecommunications Act, c. 38 (1993) (Canada); Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); and Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 10.

unrelated to the use(s) for which the individual originally disclosed their personal information.[583] Such framework also mentions that the consent shall be done in writing.[584] The party transferring the data should ensure that the third party would respect the privacy legal framework, provide the same level of privacy protection as originally chosen by the individual, and not disclose the data to any other person without the express authorization of the user.[585]

This legal framework is not specific as to who has and should have access to the wireless user's location data even if it suggests in some cases, for example in the United States, that only FCC-licensed carriers or someone under their control should have access to it. What about third parties such as *concierge* services, towing companies, and market researchers? Will private individuals be able to purchase the instant whereabouts of any person of interest? Should government control these parties' use of location data?

In the context of location-based services, the next issue to consider is what is done with the data collected through tracking. For example, a coffee company can legitimately use the tracking technology to provide a coupon to a wireless user who has agreed to receive advertising from such content provider. However, it is questionable ethics if that same information is passed on to the sporting goods store next door to send the user unsolicited advertisements about a sale on running shoes.

At the end of the day the problems related to the data transfer are mainly a *consent* issue where no party, including the LBS Provider or the carrier, is entitled to transfer location data prior to obtaining the wireless user's written consent.

---

583 *Id.*

584 Article (1) (C), The Wireless Privacy Protection Act , HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); and Bell Canada et al., *Application to Revise Article 11 of the Terms of Service*, Part VII Application to the CRTC.

585 Article 3, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Section 3, Article (b) (3), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Schedule 1, Section 5, Article 4.7.5, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002); and Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 10.

It is interesting to note that the laws do not specify if the same treatment must be given to anonymous location data. It may then be appropriate for a LBS Provider to adopt a business model and develop the technology in such a way that the transfer is impossible or at least could not be useful to a third party, as further detailed under Subsection 4.4.3.

3.6 Data Access

According to the legal framework related to the access to the data, an individual should have the right to obtain from a data controller, or otherwise and upon request, confirmation of whether or not the data controller has data relating to him.[586] The user should further have the right to have communicated to him such data within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner and in a form that is readily intelligible to him.[587] Also, an individual should have the right to challenge data relating to him and, if the challenge is successful, to have the data erased or deleted, rectified, completed or amended.[588] Furthermore, the laws mention that reasonableness of access depends on the nature and sensitivity of the information collected and its intended uses.[589]

In the context of location-based services and the collection of location data, will users have the right to inspect the location data others have gathered about them and to correct it if necessary? Will they have to pay for such access? Will the presented data be comprehensible?

---

586 Article 13 a), OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 6, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Section 3, Article (b) (1) (D), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Schedule 1, Section 5, Article 4.9, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Article 16, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada); Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); and Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 10.

587 *Id.*

588 *Id.* and Article 10 c), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

589 Article 6, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); and Section 3, Article (b) (1) (D), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

The laws do not take into account the complexity of the practical side of having wireless users access their location data, and they do not provide a different treatment for anonymous location data. The laws also do not specify what type of system a LBS Provider should provide the wireless users in order for such users to have access to their location data and update such data, as the case may be.

3.6.1 What is Considered "Reasonable Access" to Historical Location Data?

Cameroun Crouch from CNN.com in his article entitled: *Will Big Brother Track You by Cell Phone?* interviewed Mr. Averkamp from Sprint PCS[590] who confirms the U.S. carrier's view that consumers must have access to the personal data that will be used for location services.[591] This is a given, but what about access to the historical location data that is collected and stored?

The laws prescribe that an individual should have the right to have access to data relating to him in a form that is readily intelligible to him,[592] and also the right to have the data erased, rectified, completed, or amended.[593] The laws do not take into account the complexity of the practical side of having wireless users access their location data.

As a matter of fact, how is it possible to have location data provided to the wireless user in a form that is readily intelligible to him? Still to be determined is what should be considered *reasonable* access to the historical location data?

CTIA, with regards to this specific issue, has stated that in the case where the LBS Provider maintains location data as part of a customer profile, CTIA would support reasonable customer access to the profile to correct any inaccuracies, similar to the access provided to other call detail records:[594]

---

590 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

591 Cameroun Crouch, *Will Big Brother track you by cell phone?*, CNN.COM, April 20, 2001. http://www.cnn.com/2001/TECH/ptech/04/20/location.services.idg/index.html (Last accessed on July 8, 2002)

592 Article 13 b), OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980).

593 Id. and Article 10 c), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and Article 6, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 5.

594 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR

> CTIA continues to support reasonable customer access to profile information that contains location-specific attributes to ensure that it is correct and accurate. As with the other principles, however, the access requirement should not be prescriptive or inflexible. It should depend on the circumstances and follow a simple proposition – if a service provider collects, stores and intends to use location information for some future transaction, the customer should be able to access the profile to ensure that the information is accurate.[595]

Sprint PCS supports a narrower view in its comments, stating that access should mean that a customer can access his or her location preferences (e.g. default settings) currently utilized by the data collector and change those decisions to reflect the person's current requirements.[596] This seems to make more sense since, practically, it may be difficult for wireless users to access the Dynamic Profiles created by the content providers. This is mainly because these Dynamic Profiles are based on inferences made following the analysis of their historical location data and Static Profile information. For this reason, Sprint PCS's suggestion that simple access to the preference settings, which would be the information contained in the Static Profile, would be appropriate is a relevant suggestion.

3.6.2 Should There be a Different Treatment for Anonymous Location Data?

The laws do not consider the fact that location data may be made anonymous in the specific context of location-based services. With regards to this issue, the industry seems to propose a different standard for such anonymous data as further detailed under Subsection 3.1.1.1. As a matter of fact, WLIA has made the following statement, which seems to imply that the wireless user should not have access to his anonymous location data:

> (...) The customer should be provided convenient access to personally identifiable location information and the right to ask that it be corrected or deleted.[597]

This type of reasoning is in line with the proposed system further detailed under Subsection 4.6.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages.

595 *Id.* p. 10.

596 *Id.* SPRINT PCS, Reply to Comments (April 24, 2001), 16 pages, p. 15.

597 *Id.* WIRELESS LOCATION INDUSTRY ASSOCIATION, Comment (April 6, 2001), 17 pages, p. 6.

3.6.3 What Type of System should be Used for Data Access?

On the industry side, MMA members are requested to establish appropriate processes or mechanisms so that inaccuracies in PII, such as account or contact information, may be corrected and that these processes and mechanisms be simple and easy to use and provide assurance that inaccuracies have been corrected.[598]

This brings up the issue of what type of system should be used by the LBS Provider to enable the wireless users to easily have access to their data. For example, SignalSoft's Access Manager software solves this problem by enabling users to access their personal profiles using the Internet, WAP or SMS, making it easy for them to add and delete services and location permissions.[599] At the same time, it is difficult not to address the fact that the size of the screen of the wireless device may be very limiting when it comes to accessing and updating a profile.

Perhaps the proposed system for data access should involve the carrier, which party is most likely to be in charge of the relationship with the wireless user for issues already discussed under Subsection 4.1.2.

3.6.4 What should be Done with the Requests to Delete Location Data?

Finally, the industry, more specifically the MMA, has recommended that members honor requests from wireless users to delete their PII in the event that they change carriers or devices or simply unsubscribe from an advertising service.[600] This suggestion brings out the issue of what a LBS Provider should do when requested to delete profile data? Should they be obliged to delete it? Should a LBS Provider only be obliged to delete PII related to the wireless user or also anonymous location data and Static Profile information?

---

598 *Id.* WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 5.

599 Signalsoft, *SignalSoft's New Access Manager™ Provides Mobile Subscribers with Enhanced Privacy and Authentication Capabilities*, Press release, June 19, 2001. http://www.signalsoftcorp.com/newsroom/pressreleases/q2_2001/press_sgsfam.html (Last accessed on July 8, 2002)

600 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 5.

4 Translating the Legal Framework into Business Practices

Location positioning technology is inherently very sensitive in terms of data collection. The accuracy of tracking technologies can be intimidating. This pressures the owner of such technology to adopt strict self-regulation in using it, whether in the adoption of an appropriate business model or in the development of security system technology.

A LBS Provider looking to deploy a technology that would enable the providing of location-based services as of today is more likely to be looking to deploy globally or at least in more than one country. For this reason, such LBS Provider will have to comply with the laws related to the protection of personal or location data and to the protection against spam, wherever it wishes to deploy such new service.

In an ideal world, the privacy laws would be global in order to avoid the potential problem of conflicting rules once personal data from multiple sources are being merged as is suggested by author Robert Gellman in his article entitled: *Does Privacy Law Work?*:

> In the end, the complexity of the privacy issue and the multiplicity of legal responses and jurisdictions may be the key to a more rational approach. Traditional distinctions between types of records and categories of records keepers are eroding. Personal data from multiple sources are being merged through computers and computer networks. Information comes from government files, consumer transaction records, corporate files, and international sources as well. Records from some but not all of these sources come with privacy rules. These rules may not only be different; they may conflict.[601]

Since privacy laws are not the same on a global scale, a LBS Provider would have to come up with a business plan that takes into account the specific aspects of this new type of service and also deals with the disparities in the privacy laws.

---

601 Robert Gellman, *Does Privacy Law work?*, Technology and Privacy: The New Landscape, edited by Philip E. Agre and Marc Rotenberg, MIT Press, 1998, p. 193, p. 209, p. 214.

At the same time, a LBS Provider will have to ensure that its business model complies with each and every law enforceable in the area where it wishes to deploy its technology.

As Danny Weitzner from World Wide Web consortium[602] mentioned at the FTC Public Workshop on wireless privacy, location-based services will need to exist in a variety of legal environments:

> Already Europe has I think the kind of environment you might want to have, without getting into it too far, and what we see is the need for services to be able to exist in a variety of legal environments. (...) I tend to agree with you that it's not at the level of regulation.[603]

With regards to this issue, Nextel's[604] and Sprint PCS's[605] positions are also that, given the fact that the networks are built and operated in multi-state regions, carriers may as a practical matter have no choice but to adopt nationwide the requirements of the state adopting the most stringent standards.[606] For this reason, such LBS Provider may want to ensure that it is complying with laws located in the countries in which it is looking to deploy its technology. As a result, the following proposed privacy solution is based on the hypothesis that a LBS Provider is looking to deploy its technology in North America and in Europe. In this case, a LBS Provider would have to ensure that its solution complies with the stringent North American and European legal requirements, so that its technology will be considered *legal* in both these jurisdictions.

The development of an appropriate business model and the appropriate technology system should aim at solving the privacy issues resulting from location-based services that have not been addressed by the laws as of today. Such business model and technology system may also solve the fact that we do not know if these issues will be taken care of through appropriate amendments and modifications to the laws in the near future. As a matter of fact, this new type of technology is not only uncertain but is most likely to bring some changes on the legal side in the future. We simply do not know when.

---

602 http://www.w3.org/ (Last accessed on July 8, 2002)

603 Danny Weitzner, World Wide Web consortium, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 11, 2000, p. 19, 20. http://www.ftc.gov/bcp/workshops/wireless/001211.htm (Last accessed on July 8, 2002)

604 http://www.nextel.com/ (Last accessed on July 8, 2002)

605 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

606 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Comment (April 6,

Also, potential modifications to the law may not occur for a long time if we take into account that many carriers in the U.S. (including AT&T,[607] Verizon Wireless[608] and Sprint PCS[609]) have informed the FCC that they believe it is premature to adopt rules governing location privacy practices.[610] These carriers are not convinced that a rulemaking at this time would completely meet the needs of the American public.[611] Voicestream Wireless[612] has emitted a similar opinion and believes that the FCC should refrain from implementing regulations at this time.[613] Such carrier's position is based on the fact that there is a great deal of uncertainty in the marketplace with respect to how location-based services will be offered and by whom. It is further based on the fact that the FCC has not been able to predict technological development in the wireless industry any better than other industry experts. Finally, another U.S. carrier, Nextel,[614] has exactly the same opinion:

> Providers barely have begun to experiment with location-based services and the means to provide them. Attempts to craft detailed regulations are unlikely to be successful in anticipating the precise applications and potential abuses that may develop in this highly dynamic market. Lack of information regarding actual providers' relationships and practices, customers' preferences and behavior and future technology and product developments raise an unacceptable risk that the Commission's regulations would be based on invalid market predictions and would harm rather than protect consumer's interest. This lack of market evidence also makes it improbable that the Commission could tailor detailed regulations that avoid unduly burdening service providers' commercial speech, as required by the First Amendment. (...) No market failure has occurred to justify the imposition of sweeping regulation.[615]

2001), 25 pages, p. 16.

607 http://www.attws.com/ (Last accessed on July 8, 2002)

608 http://www.verizonwireless.com/ (Last accessed on July 8, 2002)

609 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

610 Emarketer.com, *US Wireless Firms Choose Opt-In to Protect Privacy*, June 6, 2001.
http://www.emarketer.com/estatnews/enews/reuters/06_05_2001.rwntz-story-bcnettechprivacywirelessdc.html (Last accessed on June 6, 2001)

611 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Comment (April 6, 2001), 25 pages, p. 2.

612 http://www.voicestream.com/ (Last accessed on July 22, 2002)

613 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, VOICESTREAM WIRELESS CORPORATION, Reply to comments (April 24, 2001), 4 pages, p. 3.

614 http://www.nextel.com/ (Last accessed on July 8, 2002)

615 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, NEXTEL COMMUNICATIONS INC.,

Other industry leaders share the same view, like NetCoalition[616] and the DMA,[617] and have urged the FCC to allow the industry to regulate itself. Jerry Cerasale, Senior Vice President for Government Affairs of the marketing group has stated that:

> Our view is that it's still very early where the applications are, therefore to try to set regulations might kill some applications we may want.[618]

Furthermore, other players in the field are of the opinion that it is premature to have a law since many practical questions have not been answered:

> So, the problem in the wireless environment regulations is very difficult, and until we can answer some fundamental questions, I think this rush to enact privacy legislation either at the state or federal level is premature, because there's a lot of questions we do not have answers to. It seems simple to have notice and choice, but when you look at what is notice and what is choice and who determines that, it becomes much more complicated. I'd love to have an easy fix. It would make my members a lot happier, but it's not a simple question to be answered, and those who think that it is really don't understand how the technology is working and what the ramifications of stopping the flow of information will have on the economy.[619]

This brings out the main issue. Not only are these laws not specific to the providing of these types of services, but the LBS Provider has to study the legal framework and take these privacy laws to a new level. A LBS Provider will have to ensure that its business model makes sense and protects the privacy of the wireless users in the best possible way. As a matter of fact, LBS Providers must evaluate the risk that growing consumer and privacy concerns—and resulting legislation—present to their business at individual, industry, and international levels.[620]

Notice (May 14, 2001), 7 pages, p. 4.

616 *Id.* NET COALITION, Reply Comments (April 24, 2001), 11 pages, p. 8.

617 http://www.the-dma.org/ (Last accessed on July 8, 2002)

618 Emarketer.com, *US Wireless Firms Choose Opt-In to Protect Privacy*, June 6, 2001.
http://www.emarketer.com/estatnews/enews/reuters/06_05_2001.rwntz-story-bcnettechprivacywirelessdc.html (Last accessed on June 6, 2001)

619 Rick Lane, Director, eCommerce and technology at the U.S. Chamber of Commerce, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 11, 2000, p. 44. http://www.ftc.gov/bcp/workshops/wireless/001211.htm (Last accessed on July 8, 2002)

LBS Providers must ultimately determine the level of risk with which they are comfortable and, perhaps most challenging of all, decide how decisions regarding privacy will impact business and Information Technology strategy and operations.

With regards to this issue, Victoria Bellotti, in her article entitled*: Design for Privacy in Multimedia Computing and Communications Environments* mentions that the privacy laws do not help the industry in designing the right system to provide these types of services:

> At the same time, codes of ethics and principles like those of the OECD represent ideal states of affairs about which claims can be made and contested in a court of law or some professional tribunal, but they do not help designers to determine what system properties will achieve them and furthermore, they do not tend to address themselves to the usability implications of mechanisms designed to protect privacy.[621]

For location-based services to work on a long-term basis, LBS Providers are going to have to translate these privacy laws into business practices, and adopt business models and privacy policies that are specific to this new context. On this issue, Evan Hendricks, Editor for The Privacy Times,[622] suggests that LBS Providers, through news programs and anecdotal evidence, offer suggestions for how the industry should approach consumer privacy[623] and advises companies to develop privacy standards into their business plans.[624]

Furthermore, companies will also have to come up with a security system that enables them to provide wireless users with location-specific services while avoiding the privacy issues. With regards to this last issue, privacy groups should be currently working with the technicians designing the standards for wireless location systems since how that standard is written has huge privacy and public policy implications. It may be possible to build location information into a range of systems that provide consumer convenience but avoid some of the surveillance, tracking, and record-keeping problems.

---

620 Arabella Hallawell, *Beyond the Headlines: Privacy Issues and the Enterprise*, GARTNER INC., May 4, 2001.

621 Victoria Bellotti, *Design for Privacy in Multimedia Computing and Communications Environments*, Technology and Privacy: The New Landscape, edited by Philip E. Agre and Marc Rotenberg, MIT Press, 1998, p. 63, p. 81.

622 http:// www.privacytimes.com (Last accessed on July 8, 2002)

623 Wireless Location Industry Association, *WLIA wireless location industry issues workshop, Wednesday, January 31, 2001 Washington, DC,* NEAR MAGAZINE, Newsletter, March 2001. http://www.wliaonline.org/publications/wliaworkshop.html (Last accessed on July 8, 2002)

A difficult challenge for any LBS Provider is to protect the wireless users from intrusive monitoring and marketing while using tracking technology to provide these consumers with this new type of personalized services. For this reason, each LBS Provider will have to take a huge leap forward in the development of a system that ensures complete privacy for every consumer in the network while using wireless tracking capabilities in order to deliver highly personalized, location-based services to wireless users.

Another challenge for a LBS Provider looking to provide location-based services is to figure out how to make an effective disclosure and obtain a meaningful consent from wireless users. Furthermore, a LBS Provider will have to determine how to collect and use quality data and how to offer a secure system that also provides access for the wireless user to his location data and prohibits data transfer to third unauthorized parties. Finally, such LBS Provider will have to come up with a business model and technology system that are compatible with privacy protections and that also comply with the present relevant laws and regulations.

As analyst Arabella Hallawell outlines in her article entitled: *Privacy Laws Abroad: How Worried Should Enterprises Be?* the details of translating these privacy laws into actual business and Information Technology practices will be the greatest challenge for enterprises and for those responsible for ensuring compliance.[625]

4.1 Effective and Full Disclosure

Carriers already use wireless users' location data in order to provide these users with telecommunications services. Still, it would still make sense for the carrier or LBS Provider using the same location data to inform the wireless user on the issues surrounding the tracking and the collection and storage of this data in the event that these activities are not part of regular telecommunications services.

Also, since location data is extremely sensitive data and, since the collected location data may either contain PII or pose the threat that it may be merged with PII, the laws regarding the protection of

---

624 *Id.*

625 Arabella Hallawell, *Beyond the Headlines: Privacy Issues and the Enterprise*, GARTNER INC., May 4, 2001.

personal data should apply to such data collection. For this reason, wireless users need to be informed of all aspects surrounding the tracking.

4.1.1 Receiver of Disclosure

As previously discussed, there are two types of consent required. The first type is related to the tracking and the collection of location data from the wireless users with all of the implications such as storage and security. The second type is related to the consent of the wireless user prior to receiving location-based services.

Regarding this last type of consent (related to receiving location-based servcices), wireless users clearly need the disclosure of the LBS Provider related to the collection of their location data, since they will provide their consent based on the LBS Provider's privacy policies.

With regards to the first type of consent (related to the tracking), there are two types of wireless users who could be tracked: the first type includes the wireless user who would be tracked on a personal basis, meaning that his identity is known, and so clearly needs to obtain the effective disclosure with regards to the tracking. On the other hand, it is not so clear if the second type, which is the wireless user who would be tracked anonymously, should also obtain a disclosure prior to the tracking. On this last issue of the anonymous tracking, it depends on the status of anonymous location data and also on which party owns this location data.

4.1.1.1 Status of Anonymous Location Data

Location data is very sensitive. Research identifies different potential threats associated with wireless location services that would result from improper handling of location data:

- The discovery and matching of location whereabouts can be used by the private sector to classify individuals, impose unwelcome marketing practices, and manipulate consumer behavior.[626]

- The disclosure of a user's whereabouts increases the scope for politically damaging and personally embarrassing situations.[627] As a matter of fact, location data may be used for activities or repression against individuals and substantially enhances the scope for blackmail and extortion. For example, persons at risk may include celebrities, dissenting thinkers, and people in sensitive jobs (i.e., prison management, judges, doctors, protected witnesses, and undercover agents, etc).[628]

- Location data may provide a wealth of circumstantial evidence for criminal cases.[629] This may negatively affect the presumption of innocence and provide a range of credible threats of conviction.[630]

- Location enhances the visibility of behavior. This increases the potential for measures against individuals, both by public and private organizations.[631] For example, frequent visits to a hospital may disclose a health problem that may be used against a job applicant.

The most important aspect about wireless technology is that each device, which usually belongs to one specific individual, transmits a unique identifier, which enables the wireless phone to communicate and identify itself as it passes from one cell to another. A breach is possible and unauthorized third parties may find ways to capture the unique identifier transmitted by wireless phones and be able to link the wireless phone's unique identifier with the true identity of the wireless phone user.

As previously mentioned, since, in the case of location-based services, there is always a threat that location data be merged with PII even if such threat is very small, it may be useful to also provide the disclosure to the wireless user prior to the tracking, whether anonymous or not. As a matter of fact, a wireless user should be disclosed with the fact that they are being tracked, especially if such tracking

---

626 Euro Beinat, *Privacy and Location-based Services: Stating the policy clearly*, GEO INFORMATICS, September 2001.

627 *Id.*

628 *Id.*

629 Roger Clarke, *Person-Location and Person-Tracking: Technologies, Risks and Policy Implications*, XAMAX CONSULTANCY PTY LTD., October 1999. http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html (Last accessed on July 8, 2002)

630 Euro Beinat, *Privacy and Location-based Services: Stating the policy clearly*, GEO INFORMATICS, September 2001.

631 *Id.*

is not directly related to the standard telecommunications services he has agreed to be part of. This reasoning is based on the fact that a reasonable wireless user who would subscribe to telecommunications services, would probably not be expecting that his every move, whether anonymous or not, be tracked and recorded. Such reasonable user would also not be expecting that his location data be kept for a period of time longer than is reasonably necessary for billing or for challenging an invoice.

4.1.1.2 Ownership of Location Data

With regards to the ownership of the location data, we appear to be in the presence of a co-ownership of such data between the carrier and the wireless user. For example, carriers are now able to do whatever they wish with location data, even transfer it to LBS Providers, if and only in the event that there is no PII associated with the location data. If there is PII associated with it, there could be a breach of privacy since it becomes personal data and regulations regarding the protection of personal data further discussed under Subsection 2.2.1 provides that the consent of the user be obtained prior to the collection or use of such data. Reuven Carlyle, VP Strategy planning at XY Point Corp.[632] seems to share a similar view:

> So the ownership of the data whether it's anonymous or not anonymous, the ownership of the data is absolutely essential, and Xypoint's position is very clear, it is absolutely unequivocally the carrier's and the consumer's data, and other application providers are not the gate keeper of that data. That doesn't mean applications don't need to have the opportunity to flourish, but it needs to be clear on ownership.[633]

The legal framework related to the transfer of personal data prescribes that individuals be given the opportunity to choose whether, and the manner in which, a third party uses the personal data they provide when such use is unrelated to the use(s) for which the individual originally disclosed it.[634]

---

632 Xypoint is now part of TeleCommunication Systems (TCS). http://www.xypoint.com/ (Last accessed on July 30, 2001), and http://www.telecomsys.com (Last accessed on July 8, 2002)

633 Reuven Carlyle, VP Strategy planning at XY Point Corp., participant at the Federal Trade Commission – Panel on location-based services and advertising: possibilities and privacy concerns, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 40. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

634 Article 26 (a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Article 3, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000).

Whatever the position regarding the ownership of the location data, the fact remains that a LBS Provider looking to provide location-based services must obtain the consent of the wireless user prior to collecting such information. The reason for this is that the purpose of the collection is, in that case, not related to the providing of standard telecommunications but the providing of new value-added services. Since the purpose of the collection is now different, the consent of the wireless user prior to the tracking is required.

4.1.2 Party Responsible for Providing the Disclosure

The party in charge of providing the disclosure to the wireless users that they are being tracked (and any related issue) should be the carriers. One of the reasons is that they provide the network service and thus already own the relationship with their subscribers.[635] CTIA also seems to agree with this reasoning:

> As described below in more detail, the Commission's rules adopting CTIA's fair location information practices would need do no more, for example, than require location service providers to inform their customers of their practices for the collection, use, disclosure and protection of location information. The manner and means of notice can and should be left to the service provider who has the direct relationship with the customer.[636]

---

http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Section 222 was again amended by The Wireless Communications and Public Safety Act, Pub. L. No. 106-81, HR 514, 106th Congress, 1st Session (1999); Schedule 1, Section 5, Article 4.7.5, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Article 13, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada); Bell Canada et al., *Application to Revise Article 11 of the Terms of Service*, Part VII Application to the CRTC, Ottawa (November 15, 2000); Bell Canada et al., *Application to Revise Article 11 of the Terms of Service*, Public Notice CRTC 2001-60-1, Ottawa (May 31, 2001). http://www.crtc.gc.ca/archive/eng/Notices/2001/PT2001-60-1.htm (Last accessed on July 8, 2002); and Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 4.

635 Donald Bromley, Fiderus Strategic Security and Privacy Services, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 11. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

636 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Comment (April 24, 2001), 21 pages, p. 6.

EPIC has the opinion that wireless users should be able to get location-based services from anyone and not necessarily from their carrier.[637] Even if this statement is relevant, perhaps the LBS Provider may have a business interest in partnering with a carrier. This would enable a LBS Provider to benefit from the trusted relationship the wireless user already has with his carrier and avoid confusing the wireless user with different parties, providing different privacy notices for different new applications. As a matter of fact, if the wireless users had to contact each service provider for each and every different service or application they had on their wireless devices, they would be very confused. Also, since the carrier already has control of the relationship, they may be viewed as the distribution channel for any new wireless service to be offered to wireless users, suggests Mark MacCarthy, Senior Vice President for Public Policy at Visa USA.[638]

Also to be considered is the fact that the sanctity of location data falls squarely into the laps of carriers who could be made the default *gatekeepers* of location data in most cases. A carrier clearly has a trusted relationship with its subscribers, whether is it following a legal or a fiduciary obligation and is in general only authorized to use subscriber information for telecommunications purposes, such as providing quality of telecommunications services, using it as billing information, and other related uses.[639] This places carriers in the position of a *trusted agent* with respect to their subscribers.

Finally, carriers generally treat customer information as a valuable asset and a trade secret. They share the customer's interest in safeguarding and protecting the information, which as a principle is without controversy.[640] Several carriers such as Sprint PCS[641] and AT&T Corporation[642] say they use the existing data on the location of a phone, which is now based on the nearest cellular tower, only to

---

637 *Id.* EPIC, Reply to Comments (April 24, 2001), 18 pages, p. 9-10.

638 Mark MacCarthy, the senior vice president for public policy at Visa USA, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 11, 2000, p. 28. http://www.ftc.gov/bcp/workshops/wireless/001211.htm (Last accessed on July 8, 2002)

639 The Telecommunications Act § 47 U.S.C. § 222 Privacy of customer information (1996); and Section 7, Telecommunications Act, c. 38 (1993) (Canada).

640 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Comment (April 24, 2001), 21 pages, p. 14.

641 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

642 http://www.att.com/ (Last accessed on July 8, 2002)

make connections and bill calls. As a matter of fact, Sprint PCS[643] has expressed the opinion that carriers have every incentive to listen carefully to what their customers want.[644] It has also mentioned that it agrees with Verizon Wireless[645] that carriers have a powerful incentive to adhere to a privacy-oriented, consumer-friendly approach to the use of personal or location data.[646] Such reasoning is based on the fact that the wireless marketplace is extraordinarily competitive and carriers that fail to maintain the trust of their subscribers will suffer severe consequences.[647]

Furthermore, in a certain report published by Computerworld, all the carriers interviewed by Computerworld said that they intended to guard that information, unless consumers wanted it used.[648]

4.1.3 Way of Providing the Disclosure

CDT proposed that, while the specific format of the company's notice may be dependent on the device used, the notice must be easy to find and understand,[649] which is in line with the legal framework relating to the disclosure.[650] CTIA pointed out in its Petition that there are several ways in which a LBS Provider could inform a wireless user about its location information practices. To name a few, it suggested that notification could be included in a service agreement prior to the commencement of services or the provider could describe its policies in electronic mail, on a website, or in a letter sent to subscribers:[651]

---

643 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

644 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Comment (April 6, 2001), 25 pages, p. 10.

645 http://www.verizonwireless.com/ (Last accessed on July 8, 2002)

646 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Reply to Comments (April 24, 2001), 16 pages, p. 10, referring to page 8 of VERIZON WIRELESS comments.

647 *Id.*

648 Matt Hamblen, *Ensuring portable privacy - Banks, retailers and airlines face the 'opt-in' issue and other challenges*, COMPUTERWORLD, December 11, 2000. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO54794,00.html (Last accessed on July 8, 2002)

649 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CENTER FOR DEMOCRACY AND TECHNOLOGY, Comment (April 24, 2001), 22 pages, p. 10.

650 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

651 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and

> There are several ways in which a service provider can inform customers about their location information practices. Notification could be included in a service agreement prior to the commencement of services. The provider could also describe location information policies in electronic mail, on a web site, or in a letter sent to subscribers. Consumers could also get notice on a bill directing subscribers to a toll-free number or Internet site address for a description of the carrier's complete policies and practices. Obviously, given the constraints associated with the size of the display on most wireless phones or other terminal equipment today, the notice requirement must fit the circumstances.[652]

Others, like Lorrie Faith Cranor from AT&T Labs Research,[653] believes that the disclosure should be made by service contracts.[654] The key findings of the Get Noticed FTC Workshop, which are useful given that they seem to take into account the type of audience of these privacy disclosures, were these notices need to be written for consumers.[655] More successful disclosures involved some common elements starting with a clear, concise statement of purpose that tells people why they should be interested in reading the document. The disclosure should take full advantage of visual design features that divide information up into pieces making it easy to find and read.[656] The drafting of effective privacy disclosures is as much of a communication challenge as a regulatory issue.

For reasons related to the size and limitations of the wireless phone screen and reasons further discussed under Subsection 3.1.3, the disclosure should not be done on the wireless device. Even if it may not be necessary to prescribe or adopt a uniform method of disclosure, the appropriate disclosure should take place at the point of sale of the carrier's store or even on the carrier's website[657] and should be made in writing,[658] using plain language instead of legalese.[659] Such disclosure should not

---

Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages, p. 9-10.

652 *Id.* p. 9.

653 http://www.research.att.com/ (Last accessed on July 8, 2002)

654 Lorrie Faith Cranor, AT&T Labs research, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 7. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

655 Howard Beales, Director, Bureau of Consumer Protection (Federal Trade Commission), *Privacy Notices and the Federal Trade Commission's 2002 Privacy Agenda*, Remarks, January 24, 2002. http://www.ftc.gov/speeches/other/privacynotices.htm (Last accessed on July 8, 2002)

656 *Id.*

657 As suggested by WLIA, in the *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

658 Articles (1) (A) and (2), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on

necessarily have to be made on paper in the case of the website consent, which would still make it a valid consent[660] according to companies like NetCoalition.[661]

4.1.4 Time of the Disclosure

The disclosure should be made prior to the collection of location data and not prior to the use, in order for such disclosure to comply with the most stringent European and North American laws and regulations[662] and avoid any potential privacy breaches.

4.1.5 Content of the Disclosure

Prior to the tracking of the wireless user and the collection of his location data and whether the wireless user will be tracked anonymously or not, the carrier should inform the wireless user of its policies with regards to the collection of the location data.[663] More specifically, the disclosure from the carrier should cover the following aspects in order to be considered appropriate, and in order to comply with all of the North American and European laws and regulations and legal framework further analyzed under Subsection 2.1:

- **The collection of the data:** The carrier should inform the wireless user of the fact that it is collecting data related to him,[664] given that such collection may not be part of the providing of

---

Energy and Commerce (2001); and Schedule 1, Section 5, Article 4.2.3, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

659 WLIA suggests that the disclosure be easy to understand, see Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

660 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, NETCOALITION, Reply Comments (April 24, 2001), 11 pages, p. 7-8.

661 NetCoalition.com is an organization committed to building user confidence in the Internet through responsible market-driven policies. http://www.netcoalition.com/ (Last accessed on July 8, 2002)

662 Article 9, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 1, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Schedule 1, Section 5, Article 4.2.3, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

663 Section 3, Article (b) (1) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

664 Article 7, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 2, U.S.

standard telecommunications services. For this reason, the consent of the wireless user prior to such collection is necessary.

- **Type of data:**[665] The carrier should inform the wireless user about the type of data being collected when the user is using his wireless device, the definition of location data, how often it is retrieved from the network depending on the tracking technology used, and the type of network, etc. As a matter of fact, if the LBS Provider does not clearly indicate to the wireless user what it is collecting from him, there is the danger of customers having exaggerated fears about the extent of the collector's knowledge. The wireless user should also be informed as to personal data that would potentially be collected and stored at the same time and as to the anonymization of the location data collected, as the case may be.

- **Way of collecting the data:**[666] The carrier should disclose to the wireless users its way of collecting the location data through the network in the case of network-based solutions or through the device in the case of handset-based solutions, as the case may be. As previously mentioned, the type of tracking technology used with relevant information related to this type of technology should be detailed and disclosed.

Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article (2), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Section 3, Article (b) (1) (B) (i), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Articles 5 (3) and 7, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002); and Article 43, Act to Establish a Legal Framework for Information Technology, Bill 161, 36th legislature, 2nd session, c. 32 (2001) (Quebec, Canada).

665 Article 6 (4) and 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002); Article 1, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article (1) (A), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Schedule 1, Section 5, Article 4.8.2 (c), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

666 Article 1, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

- **Collector's identity and place of business:**[667] The identity of the party collecting the location data, including the name and title of the person who is accountable for the organization's policies, practices, and principal place of business should be disclosed to the wireless user.

- **The quality of the collected data**:[668] A description of the type of data collected should be disclosed by the carrier in order to educate the wireless user as to the quality and accuracy of the location data. Also, the wireless user should be informed as to the steps that the organization undertakes to ensure that it is collecting data quality[669] and that it is also accurate, complete, and up to date. For example, the carrier may explain to the wireless user how it will also collect Static Profile data from the user agreeing to receive location-based services in order to enhance the quality of the collected data. Furthermore, the carrier may explain to the wireless user that he may, through the Profile Manager system (further detailed under Subsection 4.3.3), correct or update any profile data.

- **Use or purpose of the data:**[670] The carrier should specify the purpose of the location data and

---

667 Article 12, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 13, Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002); Schedule 1, Section 5, Article 4.8.2 (a), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002).

668 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

669 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 4.

670 Article 12, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 6 a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Article 6 (3) and 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002); Article 1, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article (1) (A), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Section 3, Article (b) (1) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector, 1993, c. 17; Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last

further explain how such data will be used. In the case of location-based services, the carrier should specify that such data will be used in order to profile wireless users based on their historical and behavioral location patterns (historical location data) and provide them with relevant location-based services that the users have agreed to receive. Furthermore, the carrier should undertake to inform the wireless user that he would be informed of any change in the use or purpose of the collection of the data,[671] before such change becomes effective.

- **Storage of the data:**[672] The carrier should inform the wireless users as to where the location data is located and stored, including whether any PII is stored permanently.[673] Even if the wireless user renews the authorization, he should be told how long the location data is retained before being purged.[674] The user should also be notified of the carrier's and the LBS Provider's policies regarding the storage of data[675] and the retention or processing of the data.[676]

- **Security of the data**:[677] The wireless user should be informed as to whether the data stored would be secure. More specifically, the user should obtain a statement of the organization's commitment to data security[678] and, as case may be, such statement should include the details regarding the

---

accessed on July 8, 2002).

671 Article 26 (a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Article 3, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); and Schedule 1, Section 5, Article 4.2.4, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada);

672 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

673 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 4.

674 *Id.* SIRF TECHNOLOGY INC., Notice (April 30, 2001), 14 pages, p. 9-10.

675 *Id.* CENTER FOR DEMOCRACY AND TECHNOLOGY, Comment (April 24, 2001), 22 pages, p. 10.

676 Articles 6 (4) and 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002); Section 3, Article (b) (1) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

677 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

678 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and

security measure adopted for the storage of the location data such as the type and strength of encryption. It may be interesting to note that AT&T in its Privacy Policy has been successful in adequately communicating what system and technology it uses to ensure that the collected data is secure, more specifically under the section entitled: *Network and Information Security.*[679]

- **Access to the personal data:**[680] The means for wireless users of gaining access to personal information held by the LBS Provider[681] and the system to update and correct any inaccuracy of the data collected should be disclosed to the wireless user. Also, since the LBS Provider may only use anonymous profile data, it should still inform the wireless user that it may access his Static Profile information in order to make any changes and updates through the Profile Manager. For further details related to the Profile Manager system, please refer to Subsection 4.3.3.

- **Transfer to third party:**[682] The wireless users should be informed of the identity of third parties that will potentially have access to their location data, including potential distributors of that information,[683] collectors of information, profiling and *ad serving organizations*,[684] all being types of organizations to which the carrier and LBS Provider may disclose the data. Wireless users should also be informed of these third parties' policies with regards to the disclosure of the

---

Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 4.

679 AT&T Wireless, *AT&T Wireless Privacy Policy*, Effective February 7, 2002. http://www.attws.com/privacy/ (Last accessed on July 8, 2002)

680 Section 3, Article (b) (1) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Schedule 1, Section 5, Article 4.8.2 (b), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector, 1993, c. 17; and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

681 Schedule 1, Section 5, Article 4.8.2 (b), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

682 Articles 6 (4) and 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002); Article 1, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Section 3, Article (b) (1) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Schedule 1, Section 5, Article 4.8.2 (3), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1, November 7, 2000. http://www.mmaglobal.com (Last accessed on July 8, 2002); Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard*, November 2001. http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002); and Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector, 1993, c. 17.

683 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 4.

collected data.[685] Also, what location data is made available to related organizations like subsidiaries of the LBS Provider should be disclosed to the wireless user.[686]

- **Procedure to complain**:[687] The wireless users should be informed on the system or procedure that they might use to complain about the location-based service, the carrier, the LBS Provider, content providers or other parties that may handle their location data. More specifically, the name or title and the address of the person to whom complaints or inquiries can be forwarded should be disclosed to the wireless user. Furthermore, a valid address to which the wireless user may send a request that the service or communication cease should be provided.

- **Update or change in the Privacy Policy:**[688] Furthermore, the carrier should specify that it will not change its privacy policy prior to sending either a letter or an e-mail to the wireless user entitled: *Update to the Privacy Policy*. This should be done at least thirty (30) days before the said update is intended to be effective. In the event of a change in its Privacy Policy, the carrier shall specify in the notice of update the reason for such change. Furthermore, this notice of update should specify to the wireless user on the system or procedure that they may use to unsubscribe to the service if they do not accept the new terms of the disclosure.

- **Withdraw of Consent**[689] **/ Implications of an Opt-out:**[690] The carrier should inform the individual that it may withdraw his consent at any time (subject, for example, to two (2) days notice) as well as the implications of such withdrawal. More specifically, the wireless user would be informed that when he does opt out, he is effectively opting out in several respects: (i) the user

---

684 *Id.*

685 Section 3, Article (b) (1) (A), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

686 Schedule 1, Section 5, Article 4.8.2 (e), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

687 Id. Schedule 1, Section 5, Article 4.8.2 (a); and Article 13, Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

688 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

689 Articles 6 (3) and 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002); and Schedule 1, Section 5, Article 4.3.8, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

690 Schedule 1, Section 5, Article 4.3.8, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

will no longer receive location-based messages; and (ii) he will no longer be profiled. Furthermore, all additional information provided by the user at opt-in (Static Profile information) will be deleted from the LBS Provider databases. Finally, the user should be informed that he will no longer be passively tracked by the system and that all additional location data stored in the databases will be deleted.

- **Request of deletion:** The wireless user should be informed of the procedure available to him regarding the potential request to delete his Static Profile information as well as his stored historical location data and what the carrier and the LBS Provider intend to do with such requests. More specifically, the carrier and the LBS Provider should confirm to the wireless users that they will be able at any time to request that such data be deleted through the Profile Manager system, as further detailed under Subsection 4.3.3. The carrier should further specify that upon such request, the data would be automatically deleted.

Once all of these above-mentioned issues are covered, the carrier shall provide the wireless user with the option to refuse that he be tracked for location-based service purposes.

- **Choice and consent:**[691] The choices available to a wireless user regarding the collection[692] of the location data and the choices and means the carrier or the service provider offers individuals for limiting its use and disclosure should be made clear to the wireless user. Furthermore, the method of expressing such refusal should be specified. The wireless user should be provided with the right to object, free of charge, to the processing of the data for the purposes of direct marketing[693] and

---

691 Article 1, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); and Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002).

692 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 4.

693 Article 14 b), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Articles 11 1) and 12 1), Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997); and Article 9 (2), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

to receiving unsolicited communications for such purposes.[694] More specifically, the user shall be informed that he may opt out of the tracking[695] and opt in to receiving location-based services in accordance with Subsection 4.2. Furthermore, the carrier should highlight portions of the wireless user agreement indicating that the user agrees to be located.[696]

- **Period of validity for consent**:[697] The wireless user should be informed by the carrier as to how long his consent will be valid and a carrier should keep a record of consent for as long as the permission is valid.

In the event that the wireless user agrees to being tracked and to receive location-based services after having received a disclosure from the carrier that covers the above-mentioned issues, the carrier shall inform such user whether his **responses** to the messages or **to wireless advertising** will be recorded and tracked. Especially in the case of advertising, an advertiser may, for example, be interested in knowing if a wireless user who received a location-based advertising message regarding a sales promotion responded to it and actually went to the store offering the promotion after receiving such message. Panelists from a Cahners In-Stat Group[698] survey panel of mobile phone and wireless Internet users confirmed their interest and opinion towards wireless advertising. Nearly all of these panelists wanted to ensure the privacy of any data collected on their responses to wireless advertising.[699]

---

694 Article 13, Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

695 The opt-out method is only valid if the tracking is done on an anonymous basis since the proposed solution suggests an anonymous tracking system. In the event that the tracking involves PII, the user should opt-in into such tracking.

696 Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).
http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002).

697 Article 8, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

698 Cahners In-Stat Group covers the full spectrum of digital communications research from technology to end-user, providing the analysis and perspective that allows technology vendors and service providers worldwide to make more informed business decisions. http://www.instat.com/ (Last accessed on July 8, 2002)

699 Rebecca Diercks, *Mobile Advertising: Not as Bad as You Think, Early adopters indicate reluctance, but may warm to discounts – with choice and privacy*, WIRELESS INTERNET MAGAZINE, Cahners In-Stat Group, July/August 2001.
http://www.wirelessinternetmagazine.com/news/0108/0108_research_ads.htm (Last accessed on July 8, 2002)

4.2 Choice and Consent

Once wireless users obtained an effective disclosure in accordance with Subsection 4.1, they should have the opportunity to choose whether they wish to be tracked for location-based services purposes, whether they actually wish to receive location-based messages, and to what extent.

For example, a wireless user pushed with a discount offer on his wireless device as he is walking in front of a specific store may very well appreciate the benefits of tracking. However, no one should have to feel as though his every move is watched in a *Big Brother* sense, and wireless users should be given a choice as to whether they wish to be tracked and to what level. Also, no wireless user should receive unsolicited messages on their wireless device unless such messages are anticipated.

4.2.1 Provider of Consent

Consent would come from two classes of wireless users: the first one includes wireless users who will be tracked, whether or not is it done anonymously, while the second includes wireless users who will receive advertising services on their wireless device.

It may be useful and appropriate to obtain the consent of the wireless user prior to the collection of his location data, so prior to the tracking. This is based on reasons already expressed under the introduction of Section 2, and on the fact that location data used for personalization purposes may either contain PII or at least there is a threat that location data be merged with PII since each device, which usually belongs to one specific individual, transmits a unique identifier. For this reason, a third party may find ways to capture the unique identifier transmitted by wireless phones and be able to link the wireless phone's unique identifier with the true identity of the wireless phone user.

For reasons further detailed under Subsection 4.1.2, a LBS Provider looking to provide location-based services may have to partner at some level with a carrier. For this reason and for reasons further discussed under Subsections 4.1.1.1 and 4.1.1.2, such carrier would ultimately obtain the consent from the wireless user prior to collecting and using his location data, whether such tracking is done anonymously or not.

The second class of people that need to provide their consent on all the issues further discussed under Subsection 4.2.6 and prior to receiving location-based messages includes the wireless users who will receive services and content on their wireless device in order to avoid spam.

4.2.2 Party Responsible for Obtaining the Consent

The carrier, for the reasons further explained under Subsection 4.1.2, should not only be the party providing the disclosure to the wireless users regarding the tracking but also be the party obtaining their consent related to this tracking and to the receiving of location-based services.

Robert E. Lewin, President and CEO of TRUSTe[700] agrees with the fact that the carrier may ultimately be in the best position to have a clearinghouse for anyone who wants to advertise on their network:

> I agree that we can't require the carriers to be the ultimate clearinghouse for all that information, but I would also argue that my relationship with my phone company and the various PDAs that I might use, that's my primary relationship, and in the event I receive an advertisement that I haven't requested, that I haven't opted into I would expect my carrier to get involved in that because my primary relationship from a privacy perspective is with my carrier, not with the various advertisers that I -- when I say I'm opting-in to the specific use of my data and that request isn't honored I'm going to go back to the carrier and ask them, have they sold my information to anyone. So I believe that the carrier is going to have some responsibility and ultimately may in fact be the best place to have a clearinghouse for anyone that wants to advertise on their network. There should be potentially a link to that site's privacy policy or some link to -- some way of like say an 800 number as to how you call these people directly because again that's my relationship. They're the ones that are ultimately responsible for the service I get.[701]

---

700 TRUSTe is an independent, non-profit privacy organizations whose mission is to build users' trust and confidence on the Internet. http://www.truste.org/ (Last accessed on July 8, 2002)

701 Robert E. Lewin, President and CEO, TRUSTe, participant at the Federal Trade Commission – Panel on Wireless Advertising: What forms will it take and how will disclosures be made?, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 79. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

4.2.3 Way of Obtaining the Consent

Carriers in the United States have expressed the opinion that the FCC[702] should not prescribe a uniform way to provide notice and consent. As a matter of fact, Verizon Wireless,[703] who already informs customers about its privacy policies through bill messages, website information, and advertising,[704] states the following:

> The Commission should not prescribe a uniform method or narrow range of methods for providing notice or consent. Notice and consent can be communicated effectively in any number of ways, including through a customer service agreement, through a post card or letter, in an e-mail, or over a website, orally, via shrink-wrap, or keypad response. Customers have varying needs and desires, as well as varying concerns regarding the information carriers obtain about them. Carriers must have the flexibility to tailor notice and consent practices based on these differences. For example, some consumers might want to place controls on the use of location data on a transactional basis, while others might wish to give blanket consent to the use of location data as means to ensure ready access to useful services.[705]

Sprint PCS[706] shares the same opinion and states that choosing one consent procedure over another was not a decision this Commission or any other regulatory needed to--or should--make, at least at this point in time.[707]

On the other hand, the best procedure may be that the consent be made with the carrier and at its point of sale or on its website following an effective disclosure as discussed under Subsection 4.1.5. The consent could be made in written, electronic, or other form, so long as it manifestly evidences the wireless user's desire to be tracked and to participate in the location-based services.

---

702 http://www.fcc.gov/ (Last accessed on July 8, 2002)

703 http://www.verizonwireless.com/ (Last accessed on July 8, 2002)

704 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, VERIZON WIRELESS, Comment (April 6, 2001), 12 pages, p. 5.

705 *Id.* p. 9.

706 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

707 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Comment (April 6, 2001), 25 pages, p. 9.

4.2.3.1 Push and Pull

With regards to the pull model, and as already discussed under Subsection 3.2.3.1, there is in most cases an implicit consent to the disclosing of the location. This type of consent, even if implicit, should extend only to the use of location data for that particular transaction and should not authorize any other use or disclosure without further approval by the user. In the event that the LBS Provider is storing location data gathered on the wireless user pull requests, the disclosure further discussed under Subsection 4.1.5 should be made prior to the collection of such data and consent related to such collection and storage would be required by the wireless user.

With regards to the push model, the section below will further describe the details regarding the consent that is required prior to the collection or use of location data and the receiving of location-based services.

4.2.3.2 Opt in versus Opt out

Wireless users, after obtaining a relevant disclosure as further detailed under Subsection 4.1.5, should be getting the opportunity to opt in or opt out of the tracking, depending on whether such tracking is done on an anonymous basis or not. These users should further opt in to receiving location-based messages.

4.2.3.2.1 Tracking and Collection of Location Data

Several vendors on a panel of a conference organized by the Personal Communications Industry Association[708] suggested that wireless users should be given the ability to shut off carrier collection of location data and should be taught how to do this.[709] Wireless trade groups such as the CTIA appear to be advocating a rigorous privacy standard requiring end users to opt in by agreeing to let their personal information be collected.

---

708 PCIA builds wireless communications industries. http://www.pcia.com/ (Last accessed on July 8, 2002)

709 Matt Hamblen, *Location information could invade privacy of wireless users, analysts warn*, COMPUTERWORLD, September 28, 2000. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO51388,00.html (Last accessed on July 8, 2002)

In the event that the location data gathered is linked with PII, the wireless user should be asked to opt in to such tracking after obtaining the disclosure discussed under Subsection 4.1.5. This procedure would be in line with the privacy standards advocated by wireless trade groups such as the CTIA that require end users to opt in by actively contributing to data collection.

EPIC, in its reply to comments in the Matter of the Implementation of the Telecommunications Act of 1996, has suggested that the FCC implement an opt in approach.[710] It believes that such approach is necessary to adequately protect the privacy of telecommunications customers. Attorneys General of many U.S. states provided comments to the same effect in the same Matter and are of the opinion that only opting in ensures that consumers have received and read the notice and made an affirmative decision to allow their personal information to be shared.[711]

A recent survey conducted by the American Banker's Association demonstrates that consumers either do not see or read such complicated opt-out notices or they do not understand them. Such survey found that forty-one percent (41%) of consumers did not recall receiving their opt-out notices, twenty-two percent (22%) recalled receiving them but did not read them, and only thirty-six percent (36%) reported reading the notice.[712] For this reason, such opt-out procedure may not be appropriate in the event that the tracking or collection involves PII.

On the other hand, in the event that the wireless users are being tracked anonymously, the wireless users should be, once they have obtained an effective disclosure in accordance with Subsection 4.1.5, able to opt-out of such tracking. As a matter of fact, there should be a black list for certain wireless users that may not want to be tracked by their carrier or a LBS Provider. For example, wireless users that have been a victim of stalking in the past, celebrities, politicians, and other users may simply feel uncomfortable with the idea of their historical movements being tracked and stored, even if all of this is done on an anonymous basis.

---

710 Before the Federal Communications Commission, Washington D.C., In the Matter of the Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, CC Docket 96-115 and 96-149, EPIC and other, Reply Comments (November 16, 2001), 9 pages.

711 *Id.* The Attorneys General of Alaska, Arizona, and many other U.S. states, Comments (December 21, 2001), 13 pages.

712 ABA, *ABA survey shows nearly one out of three consumers read their banks privacy notices*, Press release, June 15, 2001. http://www.aba.com/Press+Room/bankfee060701.htm (Last accessed on July 8, 2002)

It is interesting to note that the industry's position is that an opt-out procedure may also adequately protect wireless users' privacy interests. Alan Davidson, attorney for the Center for Democracy and Technology, confirmed the CDT's opinion that recommends that wireless users get the opportunity to opt out of such tracking after being notified that their location information is collected.[713] Carriers like Sprint PCS[714] seem to be of the opinion that opting out may be an appropriate solution:

> Customer consent can also be obtained using either notice/opt-in or notice/opt-out procedures. In choosing to use an opt-in procedure for itself, Sprint PCS does not mean to suggest that an opt-out procedure inadequately protects consumer privacy interests. To the contrary, Congress recently determined that a notice/opt-out procedure is an acceptable way to protect consumer privacy interests in their sensitive financial records.[715] Ensuing market experience may reveal that consumers find opt-in procedures unreasonably interfere with their ability to timely obtain and use certain desired services.[716]

The preferred solution remains the anonymization of PII, as further detailed under Subsection 4.4.3, and an opt-out procedure by the wireless user with regards to the collection his anonymized location data.

4.2.3.2.2 Receiving Location-based Services

More specifically in the case of wireless advertising, the concept of acceptance is very important to confirm that wireless messages are welcome.[717] Cahners In-Stat Group[718] recently surveyed its panel

---

713 Cameroun Crouch, *Will Big Brother track you by cell phone?*, CNN.COM, April 20, 2001. http://www.cnn.com/2001/TECH/ptech/04/20/location.services.idg/index.html (Last accessed on July 8, 2002)

714 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

715 "For example, in the 1999 Gramm-Leach-Bliley Act, Congress chose to use an opt-out procedure for sensitive financial and other nonpublic personal information. See 15 U.S.C. # 6802. Similarly the FCC, historically, used opt-out procedures for residential and small business CPNI, but it then reversed course in 1998 by imposing an opt-in requirement. See CPNI Order, 13 FCC Rcd 8061 (1998). However, the next year the 10th Circuit vacated the FCC new opt-in procedures because they impermissibly infringed upon the First Amendment. See *U S WEST* v. *FCC*, 192 F.3d 1224 (10th Cir. 1999), cert. Denied, 120 S. Ct. 2215 (2000)".

716 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Comment (April 6, 2001), 25 pages, p. 9.

717 Quios and Engage, *The Efficacy of Wireless advertising*, Industry Overview and Case Study, 2000, p. 4; and Rosalie Nelson, Neil Ward-Dutton and BG, *Wireless Marketing: Rhetoric, reality & revenues*, OVUM, Report, June 2001, p. 1.

718 http://www.instat.com/ (Last accessed on July 8, 2002)

of wireless phone and wireless Internet users to determine their interest and opinion towards wireless advertising.[719] It came to the conclusion that panelists noted the importance of having the ability to opt in for wireless advertising with fifty-eight percent (58%) of wireless phone users and seventy seven percent (77%) of wireless Internet users found it important to have this ability.[720]

The main rule is that wireless users are to be given an option to start services and given an opportunity to stop it. David Sobel, general counsel of the EPIC,[721] recently stated that we seem to be moving toward an agreement in the wireless space that the standard should be opting in, which is a process that requires active choice on the part of the wireless user to express permission.

Confirmed opt-in, also known as *double opt-in* is a process of verifying a user's permission in order to ensure that wireless push content is not accidentally or maliciously sent to the user's wireless device.[722] For example, after receiving permission from a wireless user, the LBS Provider may send a message to the wireless user to which he must positively reply in order to confirm permission to start receiving push messaging.[723]

Industry privacy associations like the WLIA,[724] the MMA,[725] and the Location Privacy Association are of the opinion that wireless users should be provided with a confirmed opt-in choice regarding the use of their location information where practicable. As a matter of fact, they seem to be promoting a confirmed opt-in approach for the wireless space in general.[726] Equipment manufacturers like

---

719 Rebecca Diercks, *Mobile Advertising: Not as Bad as You Think, Early adopters indicate reluctance, but may warm to discounts – with choice and privacy*, Wireless Internet Magazine, CAHNERS IN-STAT GROUP, July/August 2001. http://www.wirelessinternetmagazine.com/news/0108/0108_research_ads.htm (Last accessed on July 8, 2002)

720 *Id.*

721 http://www.epic.org/ (Last accessed on July 8, 2002)

722 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002)

723 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 2.

724 http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

725 http://www.waaglobal.org/ (Last accessed on July 8, 2002)

726 Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002); and Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed

Nokia[727] also seem to agree with such position:

> Consumer should be provided with a confirmed opt-in choice regarding the use of their location information where practicable. It is Nokia's view that end users must be provided with the maximum degree of choice possible as to whether they want their location information made available to the service provider or a third party for a specific transaction or whether they consent to allowing any party to store their historical personally identifiable location data for marketing or other purposes.[728]

In the event that the consent is appropriately obtained, in accordance with the present subsection, after obtaining an effective disclosure in accordance with Subsection 4.1.5, there may not be an additional need to verify the consent of the wireless user and, therefore, a double or confirmed opt-in may be useless. As a matter of fact, such double opt-in standard should probably be more relevant and should take place in a website environment when the identity of the user is unknown and anyone could have opted in on behalf of another person using his e-mail address. Such double opt-in standard would have also been relevant in the event that the consent was obtained through the wireless device but such procedure is not the best one for reasons already discussed under Subsection 3.1.3.

For these reasons, the wireless user should simply opt in to receive location-based messages. This mechanism is adequate to avoid spam and would comply with European and North American laws and regulations already discussed[729] in the event that it is obtained in accordance with Subsections 4.1 and 4.2.

Location Information Privacy Principles, WT Docket No. 01-72, LOCATION PRIVACY ASSOCIATION, Reply Comments (April 24, 2001), 12 pages, p. 5.

727 Nokia is a mobile phone supplier and a supplier of mobile and fixed telecom networks including related customer services. http://www.nokia.com/

728 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, NOKIA INC., Comment (April 6, 2001), 6 pages.

729 Articles 7 a) and 10 b), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Articles 7 and 10 a), OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); and Article 2, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002).

4.2.4 Time of the Consent

The consent of the wireless user should be obtained before the collection of location data unless such user is being tracked anonymously. In this last case, the wireless user should be informed that he is being tracked anonymously and be entitled to opt out of such tracking as soon as he is informed of such tracking.

The wireless user shall also provide his consent prior to the use of location data, meaning prior to receiving messages that are location-based. More specifically, such user will need to have opted in to a specific location-based service.

4.2.5 Duration of the Consent

The wireless user, as mentioned under Subsection 4.1.5, should be informed by the carrier as to how long his consent will be valid, and the carrier should keep a record of the user's consent for as long as the permission is valid.[730]

4.2.6 Content of the Consent

The general legal framework related to the consent is to the effect that the wireless users should provide their consent on the collection of the data,[731] the use of the data,[732] and the disclosure or

---

730 Article 8, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

731 Article 7, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 2, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article (2), The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Section 3, Article (b) (1) (B) (i), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Articles 5 (3) and 7, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002); and Article 43, Act to Establish a Legal Framework for Information Technology, Bill 161, 36th legislature, 2nd session, c. 32 (2001) (Quebec, Canada).

732 Articles 7 and 9, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Articles 6 (3) and 9 (1), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002); Article 2, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Article (2), The Wireless Privacy Protection Act , HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001); Section 3, Article (b) (1) (B) (i), The

transfer of the data to third parties.[733] Also, after receiving the disclosure further detailed under Subsection 4.1.5, the wireless users should have the right to object, free of charge, to the processing of the data for the purposes of direct marketing[734] and to receiving unsolicited communications for direct marketing purposes.[735]

At the same time and following Ovum's[736] suggestion, LBS Providers offering location-based services should give the wireless user a strong element of control over the type, frequency, and timing of advertisement delivery.[737] The wireless user's consent should further be provided on the following issues:

- **Number and frequency of messages**: The wireless users should be able to specify how many messages they wish to receive a day; including a minimum, a maximum, and a range. For example, a wireless user could agree to receive more messages on the weekend and less during the week.

Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Article 5 (3), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); Article 8, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada); Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.mmaglobal.com (Last accessed on July 8, 2002); Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001).

http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

733 Articles 7 and 9, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Section 3, Article (b) (1) (B) (i), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); and Article 5 (3), Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

734 Article 14 b), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Articles 11 1) and 12 1), Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997); and Article 9 (2), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

735 Article 13, Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

736 http://www.ovum.com/ (Last accessed on July 8, 2002)

737 Rosalie Nelson, *Mobile Advertising: building alternative revenue streams*, OVUM, Short Report 20, June 2000.

- **The provider of messages**:[738] The wireless users should be able to specify that they will accept receiving messages but only from certain content providers, even being more precise and specifying names of advertisers that could push content through their wireless device. At the same time, the user should be in a position to specify the type of content provider from which he does not wish to get messages. Cahners In-Stat Group[739] recently surveyed its panel of mobile phone and wireless Internet users to determine their interest and opinion towards mobile advertising:[740]

> However, 34 percent of mobile phone users and 43 percent of wireless Internet users said that ads would also be acceptable if no discounts were involved–if they received timely notification of certain offers such as tickets to an event going on sale. Additionally, they would like the ability, in advance, to choose the firms sending them ads.[741]

- **The type of messages**: The wireless user should be able to specify that they wish to receive a certain type of message (for example, content related to sports) and ensure that they can also specify the type of content they do not wish to receive.

- **The time of messages**: The wireless user should be able to specify that they wish to receive location-based messages only during the day, only over the weekends, etc.

- **The location of messages**: According to Ovum,[742] there should be a third type of location-based service whereby the user would specify the geographic areas from which they want to receive information and sales promotions.[743] The wireless user should be able to specify that he wishes to receive messages from certain locations. For example, he could state that he wishes to receive messages when he is downtown, or at the office, but never when he is at home.

---

738 Article 13, Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

739 http://www.instat.com/ (Last accessed on July 8, 2002)

740 Diercks Rebecca, *Mobile Advertising: Not as Bad as You Think, Early adopters indicate reluctance, but may warm to discounts – with choice and privacy*, Wireless Internet Magazine, CAHNERS IN-STAT GROUP, July/August 2001.
http://www.wirelessinternetmagazine.com/news/0108/0108_research_ads.htm (Last accessed on July 8, 2002)

741 *Id.*

742 Rosalie Nelson, *Mobile Advertising: building alternative revenue streams*, OVUM, Short Report 20, June 2000, p. 7.

743 *Id.*

The DMA[744] has compiled a draft set of guidelines relating to wireless marketing in an effort to safeguard the marketing industry from those with very little business sense, who would not hesitate to send SMS messages to recipients at all hours of the night. The guidelines make reference to the practice that any messages should clearly indicate **who the sender is,**[745] which practice seems relevant for any push message sent on a wireless device. Secondly, as already discussed, the messages sent should be **subject-relevant**. Through the use of profiling, the company should send the right message to the right person at the right time thereby increasing the efficiency of the medium and eliminating wireless spam. The wireless users should be informed **on how they may file a complaint** about the location-based service.

Finally, the wireless user needs to be able to specify **how long his consent will remain valid**[746] and **how long his location data and Static Profile data may be stored.** He should be able to request at any time that he no longer wishes to be part of such location-based service (**opt out**) and, in such case, should be entitled to request that his **location data and Static Profile data be deleted**.

4.3 Data Quality

The solution regarding the quality of the data is a combination of the appropriate tracking technology and a system that enables the wireless user to provide general profile information on a voluntarily basis (Static Profile data) as further detailed under Subsection 1.3.1. Also, the system should enable the wireless user to correct or update any data related to him in an easy way.

4.3.1 The Quality of Location Data

Location data may be considered quality data if and only if the appropriate technology is used and if the system enables wireless users who are interested in receiving location-based services to participate in the creation of their profile and to update any data relating to that profile.

---

744 http://www.the-dma.org/ (Last accessed on July 8, 2002)

745 Article 13, Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

746 Article 8, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

4.3.2 The Appropriate Type of Location Tracking Technology

The accuracy of location data will play an important role in the success of location-based services according to Reuven Carlyle, VP Strategy planning at XY Point Corp.:[747]

> The whole issue of what was discussed this morning of the difference between proximity location, which is cell site or cell sector based location and precise location, knowing the actual X and Y coordinates of a user, is extraordinarily important with respect to looking at applications as well as the development of the marketplace. A lot of studies from Forrester and others say that anywhere from 30 to 50 to 80 percent of applications will be viable just knowing the proximity of a user.[748]

Each LBS Provider adopting the same standard would facilitate the understanding of the wireless user on how the privacy protection system actually works while also promoting a general privacy standard in roaming environments. It is interesting to note that Location Interoperability Forum, a global industry initiative, was formed in September 2000 with the purpose of developing and promoting industry-common solutions for location-based services.[749]

Regarding this issue, Danny Weitzner from the World Wide Web consortium[750] suggests a common platform for providing these services:

> I think we need the consistency of a common platform like P3P, and this is true really for essentially any protocol we're talking about, I would suggest, that the user is aware of, whether it's security or privacy or any number of other things, but we clearly need more features available, and most importantly, I think we need a higher degree of control so that users are comfortable operating in an environment where they are, in fact, disclosing and relying on the disclosure of quite a bit of personal information.[751]

---

747 Xypoint is now part of TeleCommunication Systems (TCS). http://www.xypoint.com/ (Last accessed on July 30, 2002); and http://www.telecomsys.com (Last accessed on July 8, 2002)

748 Reuven Carlyle, VP Strategy planning at XY Point Corp. , participant at the Federal Trade Commission – Panel on location-based services and advertising: possibilities and privacy concerns, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000, p. 33. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

749 http://www.locationforum.org/ (Last accessed on July 8, 2002)

750. http://www.w3.org/ (Last accessed on July 8, 2002)

751 Danny Weitzner, World Wide Web consortium, participant at the Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 11, 2000, p. 18. http://www.ftc.gov/bcp/workshops/wireless/001211.htm (Last accessed on July 8, 2002)

Also, Sprint PCS[752] refers to SiRF's comments made in the context of CTIA's Petition and states that the wireless users would most likely be confused if different technologies (network-based and handset-based) were to be adopted:

> This same commenter recommends that the Commission also require carriers to identify (a) whether they use a handset – or – network-based location technology and (b) the accuracy of their location technology. However, if the Commission were to impose this requirement, Sprint PCS's customer care advocates would receive millions of calls wherein its advocates would have to attempt to explain the difference between network-based and handset-based technologies. Many customers will have difficulty understanding these differences. More fundamentally, the Commission needs to ask why consumers should be required to understand such differences. Sprint PCS is currently grappling with how to explain E911 precision to its customers, given that most customers have little understanding of cell sites, much less cell sectors and GPS technology.[753]

The type of tracking technology to be used should be analyzed for quality and accuracy of the historical location data and the real-time location data.

4.3.2.1 Historical Location Data: Network-based Method

All privacy systems have pros and cons but it is a known fact that today's network-based systems assure the most continuous tracking capability.[754] As a matter of fact, the main technology used right now for passive tracking is the network-based technology where carriers can currently derive location data by many methods including, for example, triangulating the location of the base station and antenna nearest the caller. Whenever the handset is turned on, the location data is registered with the network every fifteen or twenty minutes, depending on the network, which mechanism is also known as *passive tracking*. These network-based systems enable the accumulation of historical location databases[755] in order to provide some kind of personalization in the providing of push location-based services through Dynamic Profiling as further detailed under Subsection 1.3.2.

---

752 http://www.sprintpcs.com/ (Last accessed on July 8, 2002)

753 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Reply to Comments (April 24, 2001), 16 pages, p. 9.

754 Bourrie, Sally Ruth, *Privacy or profits?*, NEAR MAGAZINE, Vol. 1, Issue 1, May 2000, p.33.

755 *Id.*

Even though handset solutions like GPS provide the most accurate location data, they do not enable LBS Providers to gather historical location data in a passive way. Currently, the only commercial method available to passively track wireless users' location is the network solution.

On the other hand, as previously mentioned, such network-based method is not the most accurate. Handset-based technology like GPS would enable a LBS Provider to push messages to wireless users at a much more precise location in a real-time manner, even though the technology available for now does not permit that such historical data be stored and collected in this way. According to Bell Labs[756] researcher, Giovanni Vannucci, the network-based method can only *get a fix* on someone within a few thousand square feet or up to six square miles in rural areas.[757] Forrester Research feels that Cell ID's low precision would still be good enough for public sector applications like toll roads.[758] The minimum level of accuracy may be the network-based-solution Cell ID for now, but this low level of location resolution may be sufficient enough for commercial services, since a high number of tracking iterations allow statistical methods to produce reliable data. In later product versions, the LBS Provider system could connect to third party location equipment like Cell-Loc[759] or TruePosition[760] to improve accuracy.

4.3.2.2 Real-time Location Data: Handset-based Method

Handset-based solutions like GPS provide more accurate location data than any network-based method. For this reason it may be considered the preferred technology when it comes to evaluating the quality of location data. At the same time, GPS is not a reliable technology when the sky is not clear. Also, GPS satellites are not much use if the GPS receiver cannot see when the wireless user is indoors, not to mention that this technology requires handsets that are equipped with GPS.

---

756 http://www.bell-labs.com/ (Last accessed on July 8, 2002)

757 Chris Oakes, *Zeroing In on Cell-Phones 911s*, WIRED NEWS, June 30, 1999. http://www.wired.com/news/technology/0,1282,20504,00.html (Last accessed on July 8, 2002)

758 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, p. 17.

759 Cell-Loc Inc. is the developer of Cellocate, a family of network-based wireless location products that enable location-sensitive services. http://www.cell-loc.com/ (Last accessed on July 8, 2002)

760 TruePosition technology locates wireless phones, enabling wireless carriers to provide E-911 and other location-based services to wireless

4.3.2.3 Technology Solution: the Hybrid Method

The ideal method favoring the quality of both historical location data and real-time location data may be the hybrid-assisted GPS solution where GPS location information works with enhanced Cell ID technology. This would allow GPS accuracy and indoor usage that would pinpoint vertical location as well (i.e., ground floor vs. third floor).[761] This would produce extremely accurate location data--as much as GPS--but also allow for similar precision within buildings.

Gartner recently stated that within three years next-generation wireless phones would offer location services accurate to within a few meters. The technology will use a hybrid solution comprising of a combination of GPS technology and base-station triangulation located within the handset and working in conjunction with base station software:

> The problem of GPS signal strength will be largely addressed by the base station, which will provide the handset with approximate location information along with GPS satellite receiver parameters. This information will allow the handset to swiftly lock into GPS signals at low levels and report its position to within a few meters when outdoors or near a window. The base station transmissions will add another physical location point to the GPS system by means of a precise timing signal, allowing a measure of in building location. In areas with multiple base stations, usually developed areas, the handset will be able to triangulate its location from multiple base stations as well as GPS. In addition, Bluetooth-enabled handsets will provide a 2-meter to 10-meter bubble for highly localized services.[762]

Finally, and in order to obtain historical location data and enable the LBS Provider to build Dynamic Profiles of the wireless users, the wireless device would have to be designed in such a way that it would be sending out its location to the carrier or the LBS Provider on a regular basis.

---

users around the world. http://www.trueposition.com/ (Last accessed on July 8, 2002)

761 Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, p. 4.

762 Martin Reynolds, *Wireless Location Services: Who's watching You?*, GARTNER INC., May 9, 2001.
http://www3.gartner.com/DisplayDocument?id=329970&acsFlg=accessBought (Last accessed on July 8, 2002)

4.3.3 The System to Ensure that the Location Data is Quality Data: the Profile Manager

A system that would include cross-aggregation may pose privacy issues in the event that the wireless user is not involved in this process, especially given that cross-aggregation is one of the great threats computer systems pose to individual privacy.[763]

For this reason, the appropriate system would ensure that the wireless user who has agreed to receive messages also be involved in the creation of his profile, more specifically in his Static Profile as further discussed under Subsection 1.3.1. For example, a wireless user interested in receiving location-based messages may voluntarily provide personal demographic and psychographic information in order to receive personalized content based on his Static Profile.

More specifically, the wireless user, at the time that he is agreeing to receive location-based services, would have access to a web page associated with his profile (hereinafter the **Profile Manager**) through his carrier's website. The wireless user would be able to provide personal information, including gender and age, as well as personal interests, hobbies, etc. The Profile Manager would also cover all of the consent issues like the time, location, type, and frequency of messages the user wishes to receive, as further detailed under Subsection 4.2.6.

Finally, the wireless user would be able to go back to his profile and update any information at any time and also have the capability of requesting that all his profile information be deleted. Furthermore, the user may be able, through the Profile Manager, to request that his profile data (location data and Static Profile data) be deleted.

This would be possible through either online database access or an e-mail system that would allow authorized people to view their Static Profile information and make changes to it. The system would also include functions like authentication to ensure that wireless users requesting access to their Static Profile information are entitled to the information. Furthermore, the system should also comprise an auditing system that tracks access to wireless users' profile data and changes made.

---

763 *Id.*

4.3.4 The System to be Used for Updates

Since there is a practical difficulty for wireless users to update their location data, the Profile Manager system, detailed under the previous Subsection 4.3.3, could ensure that the wireless users may, at any time, go back to their Static Profile. Using the Profile Manager, wireless users would be able to specify, correct and update their personal and demographic data forming their Static Profile using an access code.

For example, a user who has agreed to receive location-based messages may realize that he is receiving messages related to hockey, based on a faulty inference made. Perhaps he entered an entertainment/sports center many times during hockey games but it was not because he is a hockey fan but because he works there. Using the Profile Manager system, such user could specify that he does not wish to receive content or advertising related to hockey when he is at that specific location (i.e., at work).

Also, the user would be able to specify the fact that he does or does not wish to receive this type of message at a specific time, at a specific location or from a certain content provider in order to enhance the quality of his profile data.

4.4 Data Security

The fundamental question regarding the security of the data is whether protection measures need to be in place and how these measures work. The LBS Provider should implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, alteration, or unauthorized disclosure or access, while also minimizing information capture and respecting the relationship of trust between carriers and their subscribers.

The industry should get away from the business model that requires the collection of personal data as much as possible. Author Victoria Bellotti, in her article entitled: *Design for Privacy in Multimedia Computing and Communications Environments* mentions that systems must instill confidence in users and that in order to satisfy this criterion, they must be understandable by these users.[764]

---

764 Victoria Bellotti, *Design for Privacy in Multimedia Computing and Communications Environments*, Technology and Privacy: The New

4.4.1 The Most Secure Tracking Technology

Some privacy advocates are of the opinion that, because the two basic tracking technologies--network-based technology and handset-based technology--have different potentials for abuse, it may be dangerous to wait until the technical standards are set to address privacy concerns.[765]

At any rate, the tracking technology to be used may not even be relevant if the data is collected with the wireless user's consent, especially if the collection is done on an anonymous basis. In either case, the wireless user can turn off his phone if he does not wish to be tracked.

4.4.2 Business Model: Partnering with Carriers to Manage the Sensitive Data

Consumer advocates and privacy groups are still ill at ease with carriers forming partnerships with content providers, fearing that content providers will be able to access a huge market of consumers, personal information included, when displaying their content to wireless subscribers. Fears of spamming, unwanted direct marketing solicitations, and data mining are problems these groups expect to face and are trying to prevent.

At best and for the above-mentioned reasons further detailed under Subsections 3.4.2.3 and 3.4.4.1, carriers can enable the provision of mobile data services but should not have a hand in delivering these services entirely themselves. Strategic partnerships with a third party may be a good way for the wireless telecommunications industry to take advantage of these new developments in wireless services.

Landscape, edited by Philip E. Agre and Marc Rotenberg, MIT Press, 1998, p. 63, 78.

765 Peter Wayner, *Technology that tracks cell phones draws fire*, N.Y. TIMES, February 23, 1998.

http://www.nytimes.com/library/tech/98/02/biztech/articles/022398track.html (Last accessed on July 8, 2002)

Carriers do have this trusted relationship with their subscribers, whether is it following legal obligations or simply because of their role as trusted third party. The fact that there is already a relationship of trust between carriers and their subscribers as well as a billing procedure puts the carriers in control of the relationship and any relationship with the subscribers.

As previously discussed under Subsections 2.5 and 4.1.2, carriers are in general only authorized to use subscriber information for telecommunications purposes, such as providing quality of telecommunications services to their subscribers, using it as billing information, and other related uses. This places carriers in the position of *trusted agent*, with respect to their customers. At the same time, the carriers know their customers' names, phone numbers, addresses and locations so it is possible that carriers in charge of managing the profiles and storing the historical location data about their subscribers in databases, etc., may be perceived to be in a conflict of interest. As a matter of fact, not only do these carriers already know the identity of the wireless users but at the same time they would know everything there is to know about the users' movements, profiles, etc.

The suggested business model that would eliminate the real or perceived conflict of interest and protect the privacy of wireless users is the following: LBS Providers would partner with carriers that already have a trusted relationship with their subscribers, as further explained under Subsection 4.1.2. This would be in line with the recent legal framework. As a matter of fact, such framework provides that the party that should have the right to process the collected location data should either be the provider of a publicly available communications service (the carrier) or a third party providing the value-added service (the LBS Provider).[766]

The carriers would only be charged with forwarding the messages to the wireless users, since they already know their name and phone number. The carriers would not be involved in the profiling or in the storage of the location data and Static profile data, even if they would be the party maintaining the relationship with the subscribers. More specifically, the carriers would provide the users with the disclosure as further detailed under Subsection 4.1, obtain their consent as further detailed under Subsection 4.2 prior to providing them with location-based services, and gather their Static Profile

766 Articles 6 (3), 6 (5) and 9 (3), Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

information through their website and the Profile Manager as further detailed under Subsection 4.3.3.

The LBS Provider only needs the location data of each wireless user as well as their Static Profile information in order to store them and be able to provide the tool to the content providers to segment the wireless users. Such tool would enable content providers to decide who they want to reach and when, based on the user's profile data. At no time do the LBS Providers actually need to know the identity of these users. For this reason, the LBS Providers would gather and store the location data through the carriers' network and store this data as well as the Static Profile information only once this information has been anonymized at the carrier level, therefore hosting a database containing only anonymized data. The security system will be further detailed under Subsection 4.4.3.

The content providers only need to know if the wireless users they are trying to reach and send messages to have the appropriate profile and are at the right time and at the right place to make the messages relevant. For this reason, LBS Providers like Profilium[767] streamline the production and management of wireless advertising campaigns by supplying their content providers' partners with a comprehensive software solution for precision targeting, efficient planning, and real-time reporting. Profilium's interface allows content providers to manage their wireless campaigns from start to finish, enabling content creation and detailed scheduling and rotations, message caps, and frequency specifications. Furthermore, campaign planners using this tool can monitor real-time statistics, conduct post-campaign analysis and track trends and response.

In the proposed solution, the content providers would be provided with a similar tool (hereinafter the **Pinpoint Tool**). Such Pinpoint Tool would enable the content providers to query the databases containing the anonymous location data as well as the Static Profile information in order to create their advertising campaigns and messages according to the profiles of the wireless users. The Pinpoint Tool will be further detailed under Subsections 4.4.3.1 and 4.4.3.2.

---

767 Profilium Inc. is a privately held company based in Montreal, Canada, that has developed wireless infrastructure solutions for a range of location-based services that enhance the mobile lifestyle and are designed to generate substantial new non-telecom revenues for carriers. http://www.profilium.com (Last accessed on July 8, 2002)

4.4.3 Technology - Security System

While it is important for technology companies including LBS Providers to develop sound privacy policies, it is more critical to ensure those standards are upheld as services are delivered to the public. Privacy policies may be good for certain aspects, like the opt-in process for example. But the real solution for protecting the privacy of wireless users in the context of personalized and push location-based services may be found, in part, in the technology and, in part, in the business model adopted and developed by LBS Providers.

The LBS Provider privacy solution should remove the possibility of a leak in PII while ensuring that no single party has access to both the PII and the profile information. The combination of network firewalls, anonymization technology, and physical separation of network tiers would ensure that even in the unlikely event that profile information falls into the wrong hands (in the case of a network or physical breach) it cannot be decrypted to discover the identity of the user. This is referred to as a *brute force* privacy system, as opposed to a policy-based privacy system, which is typical of the Internet.

The proposed technical security system is based on a technology developed by Profilium.[768] Such infrastructure solutions include a privacy system proprietary to Profilium, further detailed under Subsections 4.4.3.1 and 4.4.3.2, which would anonymize the collected location data as well as the Static Profile information at the carrier level.[769] Furthermore, such privacy system would separate what the carrier knows from what the LBS Provider knows and from what the content provider knows.[770]

4.4.3.1 Anonymizing the Collected Data

The LBS Provider's platform would ensure the privacy of wireless users by stripping all PII from the location data coming from the wireless network and the Static Profile information so that it can only use anonymous pseudonyms to identify the users.

---

768 http://www.profilium.com (Last accessed on July 8, 2002)

769 Profilium Inc., *Platform for Predictive Services*, Business Plan, Montreal, Canada, 2000.

770 *Id.*

The LBS Provider's solution that features a built-in privacy component would guarantee that no one is able to retrieve any wireless PII, such as names, telephone numbers, or addresses.[771]

The LBS Provider would enable the content providers using the Pinpoint Tool to mine the database storing the user's historical location data and the Static Profile information, in order to create psychographic and demographic profiles, through the association of user mobility data with the properties of the locale.

Since every wireless user would have been completely anonymized by the LBS Provider's encryption technology at the carrier level, the only information content providers would be exposed to is profile data relevant to forming ad campaigns and providing relevant content based on the wireless user's profile. These content providers would never be able to associate profile data characterizing the anonymous wireless users with their personal identity.

4.4.3.2 Privacy Shield Physically Separating Content Providers from Carriers

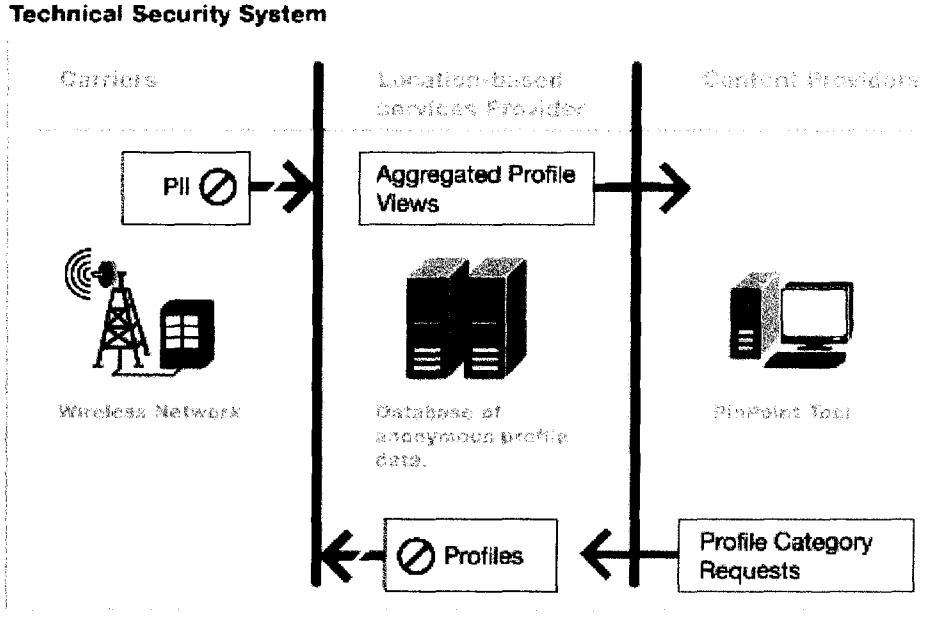
The combination of network firewalls, anonymization technology, and physical separation of network tiers would ensure that even in the unlikely event that profile information falls into the wrong hands (in the case of a network or physical breach), it cannot be decrypted to discover the identity of the user.

Carriers would be provided with a security key that would be used to encode their users' wireless phone numbers, hence avoiding all possibility that the wireless users' identities can ever be revealed to the LBS Provider, to the content providers, or to any third party. As added security, the carriers would not able to associate encoded PINs with their customers' phone numbers and PII, since the PINs would be sent directly to and stored in the LBS Provider's database.

---

771 According to article 2 a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995), "personal data" means the following: "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

FIGURE No. 3 below illustrates the mechanism of the privacy shield that physically separates content providers from carriers.



Content providers would, through the use of the Pinpoint Tool, only see an aggregated view of the user profile database, meaning that they only see a subset of the profile database. They would send queries to the LBS Provider using the Pinpoint Tool, based on profile categories such as age, sex, personal interest, or location, in order to find whether a target audience exists for a specific message.

The content providers, once they have decided on the profile they wish to target, would send a request through the LBS system to send a message, for example, to user PIN 123, if such user happens to be in a certain area at a specific time (hereinafter the **triggering event**). If the triggering event does take place, the LBS Provider system will send a notice to the carrier to send a message to PIN 123. The PIN will be decrypted at the carrier level and the carrier will send a message to the right person at the right time (only if the triggering event takes place). This way, the carrier controls the delivery, frequency and quality of the messages sent to its subscribers, ensuring that its subscribers are not spammed and are only receiving messages if they have agreed to in advance. Content providers and LBS Providers are never given access to individual user PINs, thereby further securing the system in case of breach.

With these measures, PII would be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. At the same time, the LBS Provider would, therefore, take the reasonable precautions requested legally to protect it from loss, misuse, unauthorized access or disclosure, alteration, or destruction.[772]

4.4.4 Storage Related Issues

The storage-related issues include the place where the data is stored and the identity of the people who would have access to the data, the time, and the security of the stored data.

4.4.4.1 The Place Where the Data Resides

As previously mentioned, the database would be hosted by the LBS Provider who would have no knowledge of the identity of the wireless users. As a matter of fact and as previously mentioned, the wireless user's location data and the Static Profile information would be anonymized through encryption at the carrier level.

4.4.4.2 People Who Have Access to the Data

The only people who would have access to the database containing anonymous location data and Static Profile information besides the LBS Provider would be the content providers. Still, they would not have physical access to the data and would only see an aggregate view of the user profile database, meaning they only see a subset of the profile database. They would send queries to the LBS Provider's databases using the Pinpoint Tool, based on profile categories such as age, gender, location, and personal interests, in order to find whether a target audience exists, but they would never have access to the PII of the wireless users.

---

772 In doing so, the LBS Provider complies with article 11, OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); and article 4, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002).

4.4.4.3 Time of Storage

The aggregate profile data (location data and Static Profile data) would be stored for as long as the wireless user's consent is valid, in accordance with Subsections 4.1.5, 4.2.5, and 4.2.6, or until such user requests that his profile location data be deleted. This should be a procedure easily accessible through the Profile Manager. For further details with regards to the Profile Manager, please refer to Subsection 4.3.3.

4.4.4.4 Security of the Storage

The storage is secure for the main reason that the databases contain no PII of wireless users. Author Philip E. Agre promotes the fact that databases that contain no PII do not need to be secured as tightly as databases storing PII in his article entitled: *Beyond the Mirror World: Privacy and the Representational Practices of Computing*:

> Despite their complexity, schemes based on digital pseudonyms offer certain advantages beyond the protection of individual privacy. Because databases indexed by pseudonyms no longer contain individually identifiable information, they need not be secured as tightly. Information can also be more readily transferred across organizational boundaries for purposes such as statistical research.[773]

Also, content providers who have queried the databases using the Pinpoint Tool in order to provide users with relevant location-based services have kept the anonymous profiles they have created. For this reason, the databases that only contain anonymous historical location data and Static Profile data do not have to be secured as tightly since the carrier is the one holding the key to the encryption.

The suggested type of encryption to be used would be any recognized type of encryption that has the strength of 128 bits, since such strength seems to be the strongest type of encryption that is legal, and accepted in most countries including the United States,[774] Canada,[775] and France.[776] This type of

---

773 Agre, Philip E., *Beyond the Mirror World: Privacy and the Representational Practices of Computing*, Technology and Privacy: The New Landscape, edited by Philip E. Agre and Marc Rotenberg, MIT Press, 1998, p. 29, p. 53.

774 Revised U.S. Encryption Export Control Regulations, January 2000.
http://www.epic.org/crypto/export_controls/regs_1_00.html (Last accessed on July 8, 2002)

775 Export and Import Permits Act, Aera Control List, SOR/81-543, May 12, 1999; Export and Import Permits Act, Serial No. 113, Export Controls on Cryptographic Goods, Notice to exporters, December 23, 1998; and General Export Permit No. 39 – Mass Market Cryptographic

encryption would ensure the data that is stored is also secure if one considers that it is estimated to take well over 13 billion times the age of the universe to crack a 128-bit key.[777]

Due to the fact that the LBS Provider would encrypt PII and allow limited access to aggregated profile data to third parties like content providers, it would be technically impossible to deduce a wireless user's identity by studying profile data. Furthermore, since all location data would be anonymized and no one except the carrier would have access to PII of the wireless users, a breach is essentially useless to the breaching party, hence minimizing the risk in the case of a physical or network breach.

Finally, the idea is not only to protect the stored data but also to enable the wireless users to be confident when adhering to a new location-based service, as suggested by author Philip E. Agre:[778]

> Encouraging the adoption of such technologies, unfortunately, requires more than technical existence proofs. One significant issue is trust in the system.[779]

4.5 Data Transfer

In the proposed solution, the LBS Provider system would be built upon the premise that the wireless user's privacy is best assured by physically separating the user's personal data from any third party's eyes. As a matter of fact, third parties such as content providers would only see aggregated views of profile information, views that never include PII such as names, addresses, or phone numbers. Since all location data is anonymized and no one except for the carrier has access to PII of the wireless users, a breach or a transfer is essentially useless to the breaching party. At the same time, the

---

Software, Export Permits Act, SOR/99-238, June 1999.

776 Loi no 96-659 de réglementation des télécommunications (July 26,1996) (France); Décret no 99-200 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable (March 17, 1999) (France); Décret no 99-199 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procedure de déclaration préalable est substituée à celle d'autorisation (March 17, 1999) (France); and Décret no 98-207 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procedure de declaration préalable est substituée à celle d'autorisation (March 23, 1998) (France).

777 Industry Canada, Le commerce électronique au Canada: Instaurer la confiance dans l'économie numérique, *Sécurité et cryptographie – Politique cadre en matière de cryptographie aux fins du commerce électronique*, Pour une économie et une société de l'information au Canada, December 10, 2000. http://e-com.ic.gc.ca/francais/crypto/631d13.html (Last accessed on July 8, 2002)

778 Agre, Philip E., *Beyond the Mirror World: Privacy and the Representational Practices of Computing*, Technology and Privacy: The New Landscape, edited by Philip E. Agre and Marc Rotenberg, MIT Press, 1998, p. 29.

proposed solution is to make impossible or useless a transfer of the aggregate data.

More specifically, the LBS Provider (as further detailed under Subsection 4.3.3) would encrypt all PII at the carrier level and allow limited access to aggregate profile data to third parties like content providers. This would make it technically impossible to deduce a wireless user's identity from studying profile data. The LBS Provider's profile database would only contain anonymous historical location data and demographic and psychographic information about each wireless user. But it would be devoid of any PII and personal data, such as names, addresses, or telephone numbers. Hence the wireless user is not at risk for misuse of his location data since it is not possible to relate the profile to the wireless user's identity.

For these reasons, the LBS Provider's database would never be fully transferred to any third party for the simple reason that the data would be meaningless, and thus useless, to such third parties, due to the lack of PII. This lack of PII would render the third party incapable of targeting any wireless users, since it would not know their names, wireless phone numbers, or locations.

4.6 Data Access

4.6.1 Reasonable Access to Location Data

It seems that the industry[780] has agreed on a standard with regards to the access to the data in the case of location-based services, where a written detailed profile report may be considered appropriate. Such standard proposes that the access to the Static Profile information of the wireless user, and not directly to the location data of such user, may be considered adequate access.

Furthermore, such a solution solves the practical problem resulting from providing access to wireless users to their historical location data. It enables the LBS Provider to communicate to the wireless user data relating to him in a form that is readily intelligible to him in accordance with the laws.[781]

---

779 *Id.* p. 55.

780 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Comment (April 24, 2001), 21 pages, p. 15 and 16.

781 Article 13 b), OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980).

4.6.2 Access to Anonymous Location Data

In a general way, there seems to be a different status for location data that is made anonymous, as previously discussed under Subsection 3.1.1.1. The law requires that wireless users be able to refer and have access to databases that contain some of their personal information. For this reason and since in the proposed system this data stored is anonymized, it may be irrelevant and useless to provide wireless users with such access, notwithstanding the fact that it would be very impractical to provide such access.

4.6.3 System for Data Access

The LBS Provider needs to establish an appropriate, simple, and easy mechanism so that inaccuracies in the wireless user's profile may be corrected. Such system should be included in the Profile Manager in accordance with Subsection 4.3.3.

The system should include an authentication system that would ensure that people requesting access to information gathered about them are entitled to the information and also comprise of an auditing system that automatically tracks access to consumer information and changes made.

This proposed solution is in accordance with the actual regulations and with the general principles regarding the protection of the wireless user privacy for two reasons. The first reason is that these databases contain strictly anonymous data and the law requires that the wireless users be able to refer and have access to databases that contain some of their personal information.

The second reason is that a wireless user may always refer to their Static Profile through the Profile Manager and ensure the information is accurate and updated.[782] In the event that the user has received a message that seems to imply that a content provider made an untrue inference, it may refer back to his Static Profile and ensure to restrict these kinds of messages. For more information regarding the

---

782 This complies with article 6 d), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); and article 8, OCDE, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (September 23, 1980).

update following an untrue inference, please refer to Subsection 3.3.1. Finally, such access must be provided to the wireless user, free of charge.

4.6.4 Request for Deletion of Location Data

The MMA's recommendation is that members should honor requests from wireless users to delete their PII in the event that they change carriers or devices or simply unsubscribe from the service.[783] PIPEDA prescribes that personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous.[784]

It is a given that wireless users should be able at any time to request that their PII be deleted. The proposed system should take this a step further and require that anonymous location data or Static Profile information that has never been associated with PII should also be deleted, if wireless users request it.

The Profile Manager as further detailed under Subsection 4.3.3 would provide a section where wireless users wishing to delete the information related to their Static Profile or to their anonymous location data could make such a request.

The reasoning behind this suggestion is that some wireless users may be uncomfortable with the idea that the Static Profile information and their location data, regardless of the fact that they have been anonymized and never associated with their PII, still be available and in the hands of third parties. Also, since this data will no longer be used for providing the location-based services at the request of the wireless user, there is no purpose in keeping it, and therefore should be deleted at the request of such user. Also, the data would be useless since it could never be used for another purpose without the prior consent of the wireless user, according to privacy laws.[785]

---

783 Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages, p. 5.

784 Schedule 1, Section 5, Article 4.5.3, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada).

785 Article 10 a) and b), OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980); Article 6 a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995); Article 2 and 3, U.S. Department of Commerce, *Safe Harbor Agreement* (November 1, 2000).

Conclusion

Personalized location-based services are expected to grow considerably over the next few years and location tracking capabilities will empower content providers to deliver location-based messages to wireless phone users, offering personalization at a new level.

As a matter of fact, location-based services present a unique opportunity for content providers to bridge the prediction of consumers' preferences and buying patterns with direct marketing targeted to their exact location. This relationship between the marketer and the consumer can be mutually beneficial, but its desirability and acceptability depends on the consumers' control over the messages to which they are exposed. While wireless location technologies provide a unique ability to offer valuable services to consumers, these same technologies also raise genuine concerns about the ability to locate or track wireless users against their will or send them unsolicited messages based on their geographical position.

Consumers are already dissatisfied with the volume of unsolicited marketing directed to them by mail, telephone and e-mail.[786] Consumer dissatisfaction is likely to be heightened when wireless messages arrive from third parties with whom the consumer has not established any relationship. Without awareness of how their location data is being used and who has access to it, consumers will feel as though there is omnipresent surveillance of their activities by companies they do not know. Also, an independent analysis of the competitive forces, revenue models, and wireless advertising possibilities from INSEAD revealed the fact that the mobile device is a personal tool that contains telephone numbers, and dates and that subscribers operate without expecting any disturbance to their privacy.[787] For this reason, the level of intimacy as the basis for the permissive marketing is the only way ahead.

---

http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002); Section 3, Article (b) (1) (C) (ii), The Location Privacy Protection Act, S 1164, Introduced by Sen. John Edwards, Congressional Record (2001); Schedule 1, Section 5, Article 4.2.4 and Article 4.5, Personal Information Protection and Electronic Documents Act, c. 5 (2000) (Canada); and Article 8, Act Respecting The Protection of Personal Information In The Private Sector, c.17 (1993) (Quebec, Canada).

786 In a recent survey conducted by AdTech and Talk City, 29 percent said they did not find any form of online marketing intrusive while 7 percent found some advertising to be intrusive. http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905355401&rel=true (Last accessed on July 8, 2002)

787 INSEAD, *The New Wireless Economy*, An independent Analysis of the Competitive Forces, Revenue Models and Wireless Advertising Possibilities, 2001, p. 48.

Along with the power to offer personalized location-based services comes a tremendous responsibility. For this reason, each LBS Provider will have to develop the right technology and adopt the appropriate business model in order to protect the privacy of wireless phone users while maintaining their ability to provide highly personalized location-based content.

An analysis of the present North American and European privacy framework, coming both from legal and industrial sources has helped determine how a LBS Provider should work on designing itself into a corner. Such analysis establishes how a LBS Provider may create technological platforms, adopt service models, and business models that are compatible with privacy protection.

More specifically, a LBS Provider looking to deploy a technology providing personalized location-based services should initially develop a security system that encrypts all PII at the carrier level. This would allow limited access to aggregated profile data to third parties like content providers and make it technically impossible to deduce a wireless user's identity from studying profile data. The LBS Provider's profile database would only contain anonymous historical location data and demographic and psychographic information about each wireless user, but would be devoid of any PII, such as names, addresses, or telephone numbers. Hence the wireless user would not be at risk for misuse of his location data, since it would not be possible to relate the profile to the wireless user's identity.

The LBS Provider should then look into developing the appropriate business model, which includes partnering with a carrier, in order to benefit not only from the distribution channel already in place with this carrier, but also from the trusted relationship the carrier already has with its subscribers. At this point, the carrier should be the party providing the wireless user with the disclosure and obtaining the wireless user's consent.

The disclosure should be done in writing, either through the carrier's website or at a point of sale, and should disclose all the issues surrounding the collection of the data (like the type of data collected, the collector's identity and place of business, the way of collecting the data, the quality of the collected data, the use or purpose of the data, the information related to the storage of the data, and the security of the data). Furthermore, the disclosure should also specify information related to the access by the user to the data, potential or actual transfer to third parties, the procedure to complain, the implications of an opt out and a request of deletion. It should finally inform the user on the issues

related to the choice and consent, the period of the validity for the consent, and the information related to the carrier and LBS Provider privacy policy and such policy's update mechanism.

The disclosure should be done prior to the collection of location data and prior to using such data. It should be provided to any user who will be tracked, whether such tracking is done on an anonymous basis or not. The wireless user shall then be given the opportunity to decide, through an opt-out mechanism whether it agrees to being tracked on an anonymous basis and, through an opt-in mechanism, whether it wishes to receive location-based services. The wireless user should also decide on other issues relating to such services (including the type of messages it wishes to receive, the location of such messages, the frequency and time of these messages, and the period for which his consent is valid).

In order to ensure that the collected data is quality data, the LBS Provider shall use network-based technology or a hybrid method. These methods would enable the LBS provider to collect location data in passive mode in order to enable content providers to create Dynamic Profiles about the wireless users and personalize the content based on this profile. At the same time the hybrid method would enable the LBS Provider to collect and use very accurate location data in providing its location-based services.

Furthermore, the LBS Provider, through the carrier and at the time that the wireless user opts in to receiving location-based messages, should collect basic demographic and psychographic data about the wireless user, such information being also known as Static Profile data. Such information would constitute part of the wireless user's profile information, also anonymized at the carrier level and stored with the LBS Provider.

Since all location data would be anonymized and no one except for the carrier would have access to PII of the wireless users, a breach or a transfer would be essentially useless to the breaching party, hence minimizing the risk in the case of a physical or network breach. At the same time, such system would make it impossible or useless to transfer the aggregate profile data.

Finally, the LBS Provider, through the carrier's website, would provide the wireless users with a tool known as the Profile Manager. Such tool would enable the wireless users, who have opted in to

receive personalized location-based services, to refer back to their profile information at all times and correct, amend, update, and delete any information. Using the Profile Manager, wireless users could also opt out of such service and request that all of their profile information be deleted from the LBS Provider database.

As new privacy-sensitive technologies like location-based services emerge, privacy concerns can no longer be an afterthought. Wireless privacy issues now must be addressed openly by designing products with such wireless privacy issues in mind, developing a convincing self-regulatory regime, and perhaps even getting validation from the government.

SCHEDULE "A"

DISCLOSURE

ISSUES	LEGAL FRAMEWORK	SOURCE
1- Who should be provided with the disclosure?	The subject from which personal information is collected	• Articles 9 and 12 of the OECD Guidelines • Articles 6 a) and 10 b) of Directive 95/46/EC • Article 1 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.2.3 of the Personal Information Protection and Electronic Documents Act • Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector
	The customer or the user of wireless device	• Articles 6 (4) and 9 (1) 2000 EC Proposal • Article (1) (B) of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (1) (A) of the Location Privacy Protection Act of 2001 • Cellular Telecommunications Internet Association, Petition, 22 November 2000, p. 9
	Not the customer or the user of wireless device from which anonymous location data is collected	• Article 9 (1) of 2000 EC Proposal • Section 3, Articles (b) (2) (D) and Section 3, Article (f) (1) of the Location Privacy Protection Act of 2001
2- Who should be responsible for providing the disclosure?	The data collector	• Articles 9 and 12 of the OECD Guidelines • Articles 6 a) and 10 b) of Directive 95/46/EC • Article 1 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.2 of the Personal Information Protection and Electronic Documents Act • Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector
	The carrier	• Articles 6 (4) and 9(1) 2000 EC Proposal • Article (1) (B) of the Wireless Privacy Protection Act of 2001
	The provider of location-based services	• Section 3, Article (b) (1) (A) of the Location Privacy Protection Act of 2001 • Cellular Telecommunications Internet Association, Petition, 22 November 2000, p. 9

ISSUES	LEGAL FRAMEWORK	SOURCE
3- How should the disclosure be given?	In writing	• Article (1) (A) of the Wireless Privacy Protection Act of 2001
	Orally or in writing (depending upon the way in which the information is collected)	• Schedule 1, Section 5, Article 4.2.3 of the Personal Information Protection and Electronic Documents Act
	In clear and conspicuous language	• Article 1 of the Safe Harbor Agreement • Section 3, Article (b) (1) (A) of The Location Privacy Protection Act of 2001
	Easy to find, read, and understand	• Draft WLIA Privacy Policy Standard, November 2001
	The method depends on the nature of the business	• Schedule 1, Section 5, Article 4.8.3 of the Personal Information Protection and Electronic Documents Act
	Example of disclosure: an application form	• Schedule 1, Section 5, Article 4.2.3 of the Personal Information Protection and Electronic Documents Act
	Accessible on or included with the service contract	• Draft WLIA Privacy Policy Standard, November 2001
	On wireless devices, when technically feasible	• Draft WLIA Privacy Policy Standard, November 2001
	Available on web sites	• Draft WLIA Privacy Policy Standard, November 2001
4- When should the disclosure be given?	Not later than at the time of the data collection	• Article 9 of the OECD Guidelines • Article 1 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.2.3 of the Personal Information Protection and Electronic Documents Act • Draft WLIA Privacy Policy Standard, November 2001
	Before obtaining the consent of the user for the service	• Articles 6 (4) and 9 (1), 2000 EC Proposal
	Before the disclosure to a third party or use of the collected information	• Article (1) (A) of the Wireless Privacy Protection Act of 2001 • Cellular Telecommunications Internet Association, • Petition, 22 November 2000, p. 9

ISSUES	LEGAL FRAMEWORK	SOURCE
5- What should the content of the disclosure be?	A description of what type of the information is collected	• Articles 6 (4) and 9 (1) 2000 EC Proposal • Article 1 of the Safe Harbor Agreement • Article (1) (A) of the Wireless Privacy Protection Act of 2001 • Schedule 1, Section 5, Article 4.8.2 (c) of the Personal Information Protection and Electronic Documents Act • Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
	How that information is collected	• Article 1 of the Safe Harbor Agreement
	The purposes for which personal data is collected	• Article 9 of the OECD Guidelines • Article 6 a) of Directive 95/46/EC • Article 6 (4), 2000 EC Proposal • Article 1 of the Safe Harbor Agreement • Article (1) (A) of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (1) (A) of The Location Privacy Protection Act of 2001 • Schedule 1, Section 5, Article 4.2 of the Personal Information Protection and Electronic Documents Act • Cellular Telecommunications Internet Association, Petition, 22 November 2000, p. 9
	The main purposes of the use of the collected data	• Article 12 of the OECD Guidelines • Article 10 b) of Directive 95/46/EC • Article 6 (4), 2000 EC Proposal • Article (1) (B) of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (1) (A) of The Location Privacy Protection Act of 2001 • Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector • Cellular Telecommunications Internet Association, Petition, 22 November 2000, p. 9 • Draft WLIA Privacy Policy Standard, November 2001
	The place and location where the collected information will be kept	• Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector
	Clear and specific information about its policies, practices, standards, and codes relating to the management of the collected information	• Article 12 of the OECD Guidelines • Article (1) (A) of the Wireless Privacy Protection Act of 2001 • Schedule 1, Section 5, Article 4.8.2 (d) of the Personal Information Protection and Electronic Documents Act

ISSUES	LEGAL FRAMEWORK	SOURCE
	The identity (including the name, title, and address) of the data controller or the person who is accountable for the organization's policies and practices	• Article 12 of the OECD Guidelines • Schedule 1, Section 5, Article 4.8.2 (a) of the Personal Information Protection and Electronic Documents Act • Draft WLIA Privacy Policy Standard, November 2001
	The types and identity of the organizations (related organizations or third parties) that will have access to the information	• Articles 6 (4) and 9 (1) 2000 EC Proposal • Article 1 of the Safe Harbor Agreement • Section 3, Article (b) (1) (A) of The Location Privacy Protection Act of 2001 • Schedule 1, Section 5, Article 4.8.2 (e) of the Personal Information Protection and Electronic Documents Act • Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector • Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
	The choices and means the organization offers individuals for limiting the data collection, use, and disclosure	• Article 1 of the Safe Harbor Agreement • Draft WLIA Privacy Policy Standard, November 2001
	Information relating to the retention of the data (or of the processing of the data)	• Articles 6 (4) and 9 (1) 2000 EC Proposal • Section 3, Article (b) (1) (A) of The Location Privacy Protection Act of 2001 • Draft WLIA Privacy Policy Standard, November 2001
	Information relating to the storage of the data	• Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
	The data collector's commitment to data security	• Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
	Information relating to the quality of the collected data	• Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001

ISSUES	LEGAL FRAMEWORK	SOURCE
	The means of gaining access to the collected data (and how or if it is possible to update or correct such data)	• Section 3, Article (b) (1) (A) of The Location Privacy Protection Act of 2001 • Schedule 1, Section 5, Article 4.8.2 (b) of the Personal Information Protection and Electronic Documents Act • Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector • Draft WLIA Privacy Policy Standard, November 2001
	To whom complaints or inquiries can be forwarded	• Schedule 1, Section 5, Article 4.8.2 (a) of the Personal Information Protection and Electronic Documents Act
	The possibility to withdraw the consent at any time, subject to legal or contractual restrictions and reasonable notice	• Articles 6 (3) and 9 (1) of 2000 EC Proposal • Schedule 1, Section 5, Article 4.3.8 of the Personal Information Protection and Electronic Documents Act
	The implications of the consent's withdrawal	• Schedule 1, Section 5, Article 4.3.8 of the Personal Information Protection and Electronic Documents Act
6- Of what type of change should the user be informed?	Any change in the purpose or use of the collected data (and the consent shall be obtained prior to the use)	• Article 26 (a) of Directive 95/46/EC • Article 3 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.2.4. of the Personal Information Protection and Electronic Documents Act
	Any change in the privacy policy and the reason for such change	• Draft WLIA Privacy Policy Standard, November 2001

SCHEDULE "B"

CHOICE & CONSENT

ISSUES	LEGAL FRAMEWORK	SOURCE
1- From whom do you get the consent?	The data subject	• Articles 7 and 10 a) of the OECD Guidelines • Article 7 a) of Directive 95/46/EC • Articles 6 (3) and 9 (1) 2000 EC Proposal • Article 2 of the Safe Harbor Agreement • Article 7 of the Personal Information Protection and Electronic Documents Act • Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector • Article 43 of the Act to establish a legal framework for information technology
	The customer	• Article (2) of the of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (4) (A) of the Location Privacy Protection Act of 2001
2- Who should be responsible for obtaining the consent?	The data collector	• Articles 7 and 10 a) of the OECD Guidelines • Article 7 a) of Directive 95/46/EC • Articles 6 (3) and 9 (1) 2000 EC Proposal • Article 2 of the Safe Harbor Agreement • Article 7 of the Personal Information Protection and Electronic Documents Act • Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector
	The Location service provider	• Article (2) of the of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (4) (A) of the Location Privacy Protection Act of 2001
3- How should the consent be obtained?	May be done in writing, through an electronically signed service agreement or other contractual instrument	• Section 3, Article (b) (4) (A) of the Location Privacy Protection Act of 2001 • Cellular Telecommunications Internet Association, Petition, 22 November 2000
	May be done orally	• Cellular Telecommunications Internet Association, Petition, 22 November 2000
	May be done through indigenous technological mechanisms available	• Section 3, Article (b) (4) (A) of the Location Privacy Protection Act of 2001 • Mobile Marketing Association, Guidelines on Privacy and Spam • Cellular Telecommunications Internet Association, Petition, 22 November 2000

ISSUES	LEGAL FRAMEWORK	SOURCE
	An opt-out procedure (minimum requirement)	• Article 2 of the Safe Harbor Agreement • Article 7 (2), Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce • Section 5, (a) (5), Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act of 2001 • Section 2 (a) (2), The Netizens Protection Act of 2001 • Section 5 (a) (3), The Unsolicited Commercial Electronic Mail Act of 2001
	An opt-in procedure	• European Coalition Against Unsolicited Commercial Email • Section 2 (5) and Section 3 (a) (1) (e) of The Wireless Telephone Spam Protection Act of 2001 • Article 12, Personal Information Protection and Electronic Documents Act • Draft WLIA Privacy Policy Standard, November 2001
	A confirmed opt-in procedure	• Mobile Marketing Association, Guidelines on Privacy and Spam
	Depends on the circumstances	• Schedule 1, Section 5, Articles 4.3.4 and 4.3.6 of the Personal Information Protection and Electronic Documents Act
	Depends on the type of information collected and the sensitivity of such information	• Schedule 1, Section 5, Articles 4.3.4 and 4.3.6 of the Personal Information Protection and Electronic Documents Act
	Be able to opt out at any time from the tracking or the service (provided with procedures to do so)	• Draft WLIA Privacy Policy Standard, November 2001
4- When should the consent be obtained?	Before collecting the location information	• Article (2) of the of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (1) (B) (i) of the Location Privacy Protection Act of 2001 • Schedule 1, Section 5, Article 4.3 of the Personal Information Protection and Electronic Documents Act • Article 43 of the Act to establish a legal framework for information technology.
	Before processing the data	• Article 7 a) of Directive 95/46/EC • Articles 6 (3) and 9 (1) 2000 EC Proposal

ISSUES	LEGAL FRAMEWORK	SOURCE
	Before using the data	• Article 2 of the Safe Harbor Agreement • Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector • Mobile Marketing Association, Guidelines on Privacy and Spam
5- What should be the content of the consent?	The collection of the data	• Article 7 of the OECD Guidelines • Article 2 of the Safe Harbor Agreement • Article (2) of the of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (1) (B) (i) of the Location Privacy Protection Act of 2001 • Articles 5 (3) and 7 of the Personal Information Protection and Electronic Documents Act • Draft WLIA Privacy Policy Standard, November 2001 • Article 43 of the Act to establish a legal framework for information technology
	The use of the data for a specific purpose	• Articles 7 and 9 of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data • Articles 6 (3) and 9 (1) 2000 EC Proposal • Article 2 of the Safe Harbor Agreement • Article (2) of the of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (1) (B) (i) of the Location Privacy Protection Act of 2001 • Article 5 (3) of the Personal Information Protection and Electronic Documents Act • Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector • Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
	The disclosure or transfer of the collected data to third or unauthorized parties	• Articles 7 and 9 of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data • Section 3, Article (b) (1) (B) (i) of the Location Privacy Protection Act of 2001 • Article 5 (3) of the Personal Information Protection and Electronic Documents Act
	The right to object, free of charge, to the processing of personal data for the purposes of direct marketing	• Article 14 b) of Directive 95/46/EC • Articles 11 1) and 12 1) of Directive 97/66/EC • Article 9 (2) of 2000 EC Proposal

ISSUES	LEGAL FRAMEWORK	SOURCE
	The right to refuse unsolicited communications for direct marketing purposes and extended to cover all forms of electronic communications	• Article 13 of 2000 EC Proposal
	The retaining of the location information	• Section 3, Article (b) (1) (B) (i) of the Location Privacy Protection Act of 2001
	The storage of the location information	• Draft WLIA Privacy Policy Standard, November 2001
	The time for which the consent is valid or the length of time needed to achieve the purposes for which it was requested	• Article 8 of the Act Respecting The Protection of Personal Information In The Private Sector
6- What should be the content of a message?	The identity of the sender on whose behalf the communication is made	• Article 13 of 2000 EC Proposal
	A valid address to which the recipient may send a request that such communications cease	• Article 13 of 2000 EC Proposal
7- Should the consent be required if the data used is anonymized?	Where location data can be processed, such data may only be processed when they are made anonymous	• Article 9 (1) of 2000 EC Proposal
	The collection, use, retention, disclosure of, or access to, a customer's location information without prior notice or consent is acceptable to the extent necessary to produce information from which individual customer identities have been removed	• Section 3, Article (b) (2) (D) and Section 3, Article (f) (1) of the Location Privacy Protection Act of 2001

SCHEDULE "C"

DATA QUALITY

ISSUES	LEGAL FRAMEWORK	SOURCE
1- What is quality data?	The data used should be relevant to the purposes for which they are to be used	• Article 8 of the OECD Guidelines • Article 6 c) of Directive 95/46/EC • Article 5 of the Safe Harbor Agreement
	The data used should be accurate (reasonable measures should be taken to make sure the data is accurate)	• Article 8 of the OECD Guidelines • Article 6 d) of Directive 95/46/EC • Article 5 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.6, Personal Information Protection and Electronic Documents Act • Article 11, Act Respecting The Protection of Personal Information In The Private Sector • Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
	The data used should be complete	• Article 8 of the OECD Guidelines • Article 5 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.6, Personal Information Protection and Electronic Documents Act • Mobile Marketing Association, Guidelines on Privacy and Spam
	The data used should be kept up-to-date	• Article 8 of the OECD Guidelines • Article 6 d) of Directive 95/46/EC • Article 5 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.6, Personal Information Protection and Electronic Documents Act • Article 11, Act Respecting The Protection of Personal Information In The Private Sector • Mobile Marketing Association, Guidelines on Privacy and Spam
	The data collected must be kept in a form which permits identification of data subjects	• Article 6 e) of Directive 95/46/EC
	The data collected must be obtained from reliable sources	• Mobile Marketing Association, Guidelines on Privacy and Spam

SCHEDULE "D"

DATA SECURITY

ISSUES	LEGAL FRAMEWORK	SOURCE
1- Against what should the collected data be protected?	Accidental loss or theft	• Article 11 of the OECD Guidelines • Article 17 1) of Directive 95/46/EC • Article 4 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.7.1, Personal Information Protection and Electronic Documents Act • Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
	Unauthorised disclosure or access	• Article 11 of the OECD Guidelines • Article 17 1) of Directive 95/46/EC • Article 4 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.7.1, Personal Information Protection and Electronic Documents Act • Draft WLIA Privacy Policy Standard, November 2001
	Accidental or unlawful destruction	• Article 11 of the OECD Guidelines • Article 17 1) of Directive 95/46/EC • Article 4 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.7.1, Personal Information Protection and Electronic Documents Act
	Modification and alteration	• Article 11 of the OECD Guidelines • Article 17 1) of Directive 95/46/EC • Article 4 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.7.1, Personal Information Protection and Electronic Documents Act • Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
	All other unlawful forms of processing (where the processing involves the transmission of data over a network)	• Article 17 1) of Directive 95/46/EC
	Copying	• Schedule 1, Section 5, Article 4.7.1, Personal Information Protection and Electronic Documents Act

ISSUES	LEGAL FRAMEWORK	SOURCE
	Use or misuse	• Article 4 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.7.1, Personal Information Protection and Electronic Documents Act • Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
2- What should the methods of protection include?	Reasonable security measures	• Article 4 of the Safe Harbor Agreement • Article (3) of the of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (1) (D) of the Location Privacy Protection Act of 2001 • Schedule 1, Section 5, Article 4.7, Personal Information Protection and Electronic Documents Act • Article 10, Act Respecting The Protection of Personal Information In The Private Sector • Mobile Marketing Association, Guidelines on Privacy and Spam • Cellular Telecommunications Internet Association, Petition, 22 November 2000, p. 10 • Article 11 of the OECD Guidelines • Draft WLIA Privacy Policy Standard, November 2001
	Organizational measures (for example, security clearances and limiting access on a *need-to-know* basis)	• Article 17 1) of Directive 95/46/EC • Schedule 1, Section 5, Article 4.7.3, Personal Information Protection and Electronic Documents Act
	Technological measures (for example, the use of passwords and encryption)	• Article 17 1) of Directive 95/46/EC • Schedule 1, Section 5, Article 4.7.3, Personal Information Protection and Electronic Documents Act
	Physical measures (for example, locked filing cabinets and restricted access to offices)	• Schedule 1, Section 5, Article 4.7.3, Personal Information Protection and Electronic Documents Act
3- What are the issues to consider for a reasonable security system?	The state-of-the-art systems and the cost of their implementation	• Article 17 1) of Directive 95/46/EC
	The method of storage of the information	• Schedule 1, Section 5, Article 4.7.2, Personal Information Protection and Electronic Documents Act

ISSUES	LEGAL FRAMEWORK	SOURCE
	The nature and the sensitivity of the data to be protected	• Article 17 1) of Directive 95/46/EC • Schedule 1, Section 5, Article 4.7.2, Personal Information Protection and Electronic Documents Act
	The format of the information	• Schedule 1, Section 5, Articles 4.7.1 and 4.7.2, Personal Information Protection and Electronic Documents Act
	The amount of information collected	• Schedule 1, Section 5, Article 4.7.2, Personal Information Protection and Electronic Documents Act
	The distribution of the information	• Schedule 1, Section 5, Article 4.7.2, Personal Information Protection and Electronic Documents Act
4- For how long should the data be kept?	The telecommunications traffic data should be erased or made anonymous as soon as the communication ends	• Article 6 (1) of Directive 97/66/EC
	The telecommunications traffic data should only be kept for the purpose of subscriber billing and interconnection payments, but only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued	• Article 6 (2) of Directive 97/66/EC
	For the time necessary to accomplish the purpose (for the duration necessary for the services)	• Article 6 (3) 2000 EC Proposal • Draft WLIA Privacy Policy Standard, November 2001
5- Who should have the right to process the collected location data?	Provider of a publicly available electronic communications service	• Articles 6 (3) and 9 (3) 2000 EC Proposal
	Persons acting under the authority of providers of the public communications networks and publicly available electronic communications services	• Articles 6 (5) and 9 (3) 2000 EC Proposal
	Third party providing the value added service	• Article 9 (3) 2000 EC Proposal

SCHEDULE "E"

DATA TRANSFER

ISSUES	LEGAL FRAMEWORK	SOURCE
1- What are the obligations prior to the data transfer?	The data subject must have given his consent to the transfer unambiguously	• Article 26 (a) of the European Union Directive 95/46/EC • Article 3 of the Safe Harbor Agreement • Article (1) (C) of the of the Wireless Privacy Protection Act of 2001 • Section 3, Article (b) (3) of S 1164, Location Privacy Protection Act of 2001 • The Telecommunications Act of 1996, 47 U.S.C. Section 222 Privacy of customer information and The Communications Act of 1934, 47 U.S.C. • Article 13, Act Respecting The Protection of Personal Information In The Private Sector • Section 7, Telecommunications Act • Mobile Marketing Association, Guidelines on Privacy and Spam • Cellular Telecommunications Internet Association, Petition, 22 November 2000, p. 10
	If the use is unrelated to the use(s) for which the individual originally disclosed personal information	• Article 3 of the Safe Harbor Agreement
	In writing what information may be shared or sold to other companies and third parties	• Article (1) (C) of the of the Wireless Privacy Protection Act of 2001 • Bell Canada et al. *Application to Revise Article 11 of the Terms of Service*, Part VII Application to the CRTC
2- What are the obligations of the party transferring the collected data?	Ensure that these privacy standards are adopted and/or made a condition of doing business with third party recipients	• Draft WLIA Privacy Policy Standard, November 2001
	Care shall be used in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information	• Schedule 1, Section 5, Article 4.7.5, Act Respecting The Protection of Personal Information In The Private Sector
3- What are the obligations of third parties receiving the collected data?	Provide at least the same level of privacy protection as originally chosen by the individual Not disclose or permit access to such information to any other person without the express authorization of the customer	• Article 3 of the Safe Harbor Agreement • Section 3, Article (b) (3) of the Location Privacy Protection Act of 2001 • Cellular Telecommunications Internet Association, Petition, 22 November 2000, p. 10 • Draft WLIA Privacy Policy Standard, November 2001

SCHEDULE "F"

DATA ACCESS

ISSUES	LEGAL FRAMEWORK	SOURCE
1- What does the data subject have the right to have communicated to him?	Data relating to him / Confirmation of whether or not the data controller has data relating to him	• Article 13 a) of the OECD Guidelines
	Within a reasonable time	• Article 13 a) of the OECD Guidelines
	At a charge, if any, that is not excessive	• Article 13 a) of the OECD Guidelines
	In a reasonable manner	• Article 13 a) of the OECD Guidelines
	In a form that is readily intelligible to him	• Article 13 a) of the OECD Guidelines
2- How must the data subject have access to such data?	In a reasonable way	• Article 6 of the Safe Harbor Agreement • Section 3, Article (b) (1) (D) of the Location Privacy Protection Act of 2001 • Cellular Telecommunications Internet Association, Petition, 22 November 2000, p. 10
	Upon request	• Schedule 1, Section 5, Article 4.9, Personal Information Protection and Electronic Documents Act • Article 16, Act Respecting The Protection of Personal Information In The Private Sector
	Though appropriate and easy-to-use processes or mechanisms	• Mobile Marketing Association, Guidelines on Privacy and Spam
	Depending on the nature and sensitivity of the information collected	• Article 6 of the Safe Harbor Agreement
	Depending on the intended uses of the information collected	• Article 6 of the Safe Harbor Agreement

ISSUES	LEGAL FRAMEWORK	SOURCE
3- To what must the data subject have the right?	Verify the accuracy and challenge data relating to him	• Article 13 a) of the OECD Guidelines • Section 3, Article (b) (1) (D) of the Location Privacy Protection Act of 2001 • Schedule 1, Section 5, Article 4.9, Personal Information Protection and Electronic Documents Act • MMA, Guidelines on Privacy and Spam • CTIA Petition, 22 November 2000, p. 10
	Have the data erased or deleted (in some cases, if the users terminate their subscriptions to the location-based service)	• Article 13 a) of the OECD Guidelines • Section 3, Article (b) (1) (D) of the Location Privacy Protection Act of 2001 • Mobile Marketing Association, Guidelines on Privacy and Spam • Draft WLIA Privacy Policy Standard, November 2001
	Have the data rectified	• Article 13 a) of the OECD Guidelines • Article 10 c) of Directive 95/46/EC • Article 6 of the Safe Harbor Agreement • Article 16, Act Respecting The Protection of Personal Information In The Private Sector • Mobile Marketing Association, Guidelines on Privacy and Spam • CTIA Petition, 22 November 2000, p. 10
	Have the data completed	• Article 13 a) of the OECD Guidelines • Schedule 1, Section 5, Article 4.9, Personal Information Protection and Electronic Documents Act
	Have the data amended	• Article 13 a) of the OECD Guidelines • Article 6 of the Safe Harbor Agreement • Schedule 1, Section 5, Article 4.9, Personal Information Protection and Electronic Documents Act

BIBLIOGRAPHY

1- Legal framework

International:

OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (September 23, 1980).

Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1 (November 7, 2000). http://www.waaglobal.org/ (Last accessed on July 8, 2002)

Mobile Marketing Association, *Location Privacy Guidelines*, Draft (November 2001).

Wireless Location Industry Association, *Draft WLIA Privacy Policy Standard* (November 2001). http://www.wliaonline.org/indstandard/privacy.html (Last accessed on July 8, 2002)

Europe:

Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (October 24, 1995).

Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, European Union (December 15, 1997).

Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, European Union (2000).

Commission of the European Communities, *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* (presented to the Commission), Legislation under preparation, COM (2000) 385 Final, 2000/0189 (COD), Brussels (July 12, 2000).

Council of the European Union, *Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 15396/2/01, Brussels (January 29, 2002).

European Parliament, *II Recommendation for second reading on the Council common position for adopting a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector*, Committee on Citizen's Freedoms and Rights, Justice and Home Affairs, Final (April 22, 2002).

France:

Loi no 96-659 de réglementation des télécommunications (July 26, 1996).

Décret no 98-207 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation (March 23, 1998).

Décret no 99-200 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable (March 17, 1999).

Décret no 99-199 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation (March 17, 1999).

United States:

The Communications Act § 47 U.S.C. § 222 Privacy of customer information (1934).

The Telecommunications Act § 47 U.S.C. § 222 Privacy of customer information (1996).

The Wireless Communications & Public Safety Act, Pub. L. No. 106-81 § 113 Stat. 1288 (1999).

The Wireless Communications and Public Safety Act, 106th Congress, 1st Session (1999).

Revised U.S. Encryption Export Control Regulations (January 2000).

United States Department of Commerce, *Safe Harbor Agreement* (November 1, 2000). http://www.export.gov/safeharbor/ (Last accessed on July 8, 2002)

The Anti-Spamming Act, H.R. 718, 107th Congress, 1st Session (2001).

The Anti-Spamming Act, H.R.1017, 107th Congress, 1st Session (2001).

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act, S. 630, 107th Congress, 21st Session (2001).

Gramm-Leach-Bliley Act § 15 U.S.C. § 6803 (2001).

The Location Privacy Protection Act on S. 1164, Introduced by Sen. John Edwards, Congressional Record (2001).

The Netizens Protection Act, H.R. 3146, 107th Congress, 1st Session (2001).

The Unsolicited Commercial Electronic Mail Act, H.R. 95, 107th Congress, 1st Session (2001).

The Wireless Privacy Protection Act, HR 260, Introduced by Mr. Frelinghuysen and referred to the Committee on Energy and Commerce (2001).

The Wireless Telephone Spam Protection Act, H. R. 113, 107th Congress, 1st Session (2001).

Canada:

Canadian Standard Association, *Privacy Code a must for global economy*, Focus (Spring 1992).

Telecommunications Act, c. 38 (1993).

Canadian Standards Association, CSA Standard CAN/CSA-Q30-96, *Model Code for the Protection of Personal Information*, A National Standard (March 1996).

Export and Import Permits Act, Serial No. 113, *Export Controls on Cryptographic Goods*, Notice to exporters (December 23, 1998).

Export and Import Permits Act, Aera Control List, SOR/81-543 (May 12, 1999).

General Export Permit No. 39 – Mass Market Cryptographic Software, Export Permits Act, SOR/99-238 (June 1999).

Personal Information Protection and Electronic Documents Act, c. 5 (2000).

Quebec:

Act Respecting The Protection of Personal Information In The Private Sector, c. 17 (1993).

Act to Establish a Legal Framework for Information Technology, Bill 161, 36th legislature, 2nd session, Chapter 32 (2001).

2- Jurisprudence, Administrative Documents and Proceedings

Before the Federal Trade Communications Commission, Washington, D.C., 20554, In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, ELECTRONIC PRIVACY INFORMATION CENTER, ELECTRONIC FRONTIER FOUNDATION and THE AMERICAN CIVIL LIBERTIES UNION, Comments (December 14, 1998).

1267632 Ontario Inc. v. *Nexx Online Inc.*, Ontario Superior Court (July 9, 1999).

United States Telecom Association, EPIC, American civil liberties union v. Federal Communications Commission (FCC), On petition for review of an order of the FCC, ELECTRONIC PRIVACY INFORMATION CENTER, ELECTRONIC FRONTIER FOUNDATION and THE AMERICAN CIVIL LIBERTIES UNION, Reply Brief (April 4, 2000).

Bell Canada et al., *Application to Revise Article 11 of the Terms of Service*, Part VII Application to the CRTC, Ottawa (November 15, 2000).

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Petition (November 22, 2000), 12 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, Policy Division, FCC, Public Notice (March 16, 2001), 2 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT SPECTRUM, L.P., SPRINT PCS, Motion (March 26, 2001), 4 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS TELECOMMUNICATIONS BUREAU, Public Notice (April 5, 2001), 1 page.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, AT&T WIRELESS SERVICES, INC., Comment (April 6, 2001), 10 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CENTER FOR DEMOCRACY & TECHNOLOGY, Comment (April 6, 2001), 13 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CINGULAR WIRELESS, Comment (April 6, 2001), 6 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, DIRECT MARKETING ASSOCIATION, Comment (April 6, 2001), 6 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, DOBSON COMMUNICATIONS CORPORATION, Comment (April 6, 2001), 6 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, ELECTRONIC PRIVACY INFORMATION CENTER, Comment, (April 6, 2001), 4 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, ERICSSON INC., Comment (April 6, 2001), 4 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, GRAYSON WIRELESS, a Division of Allen Telecom Inc., Comment (April 6, 2001), 4 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, LEAP WIRELESS INTERNATIONAL, INC., Comment (April 6, 2001), 7 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, LOCATION PRIVACY ASSOCIATION, Comment (April 6, 2001), 18 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, NOKIA INC., Comment (April 6, 2001), 6 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, PERSONAL COMMUNICATIONS INDUSTRY ASSOCIATION, Comment, (April 6, 2001), 9 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, THE RURAL TELECOMMUNICATIONS GROUP, Comment (April 6, 2001), 4 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SCC COMMUNICATIONS CORP., Comment (April 6, 2001), 5 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SIRF TECHNOLOGY, INC., Comment (April 6, 2001), 11 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Comment (April 6, 2001), 25 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, THE TEXAS 9-1-1 AGENCIES, Comment (April 6, 2001), 5 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, TRUEPOSITION, INC., Comment (April 6, 2001), 17 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, VERIZON WIRELESS, Comment (April 6, 2001), 12 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS ADVERTISING ASSOCIATION, Comment (April 6, 2001), 8 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS CONSUMERS ALLIANCE, INC., Comment (April 6, 2001), 8 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS LOCATION INDUSTRY ASSOCIATION, Comment (April 6, 2001), 17 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, VERIZON WIRELESS, Notice (April 13, 2001), 3 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, AMERICAN AUTOMOBILE ASSOCIATION, Reply to Comments (April 24, 2001), 9 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION, Comment (April 24, 2001), 21 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CENTER FOR DEMOCRACY AND TECHNOLOGY, Comment (April 24, 2001), 22 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, CINGULAR WIRELESS LLC, Reply to Comments (April 24, 2001), 4 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, EPIC, Reply to Comments (April 24, 2001), 18 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, INTELLIGENT TRANSPORTATION SOCIETY OF AMERICA, Reply Comments (April 24, 2001), 16 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, LOCATION PRIVACY ASSOCIATION, Reply Comments (April 24, 2001), 12 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, NATIONAL EMERGENCY NUMBER ASSOCIATION, Reply Comments (April 24, 2001), 4 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, NET COALITION, Reply Comments (April 24, 2001), 11 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SPRINT PCS, Reply to Comments (April 24, 2001), 16 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, UNITED STATES CELLULAR CORPORATION, Reply to Comments (April 24, 2001), 8 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, U.S. DEPARTMENT OF TRANSPORTATION, Reply Comments (April 24, 2001), 5 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, WIRELESS LOCATION INDUSTRY ASSOCIATION, Reply Comments (April 24, 2001), 5 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, VOICESTREAM WIRELESS CORPORATION, Reply to comments (April 24, 2001), 4 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, ONSTAR CORPORATION, Notice (April 27, 2001), 2 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, SIRF TECHNOLOGY, INC., Notice (April 30, 2001), 14 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, NEXTEL COMMUNICATIONS, INC., Notice (May 14, 2001), 7 pages.

Bell Canada et al., *Application to Revise Article 11 of the Terms of Service*, Public Notice CRTC 2001-60-1, Ottawa (May 31, 2001) http://www.crtc.gc.ca/archive/eng/Notices/2001/PT2001-60-1.htm (Last accessed on July 8, 2002)

U.S. West Inc. v. *Federal Communications Commission*, and United States of America, United States Court of Appeals, Tenth Circuit No 98-9518, On petition for review of an order of the Federal Communications Commission (FCC 98-27) (August 18, 1999).

Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding Proposed Location Information Privacy Principles, WT Docket No. 01-72, INTELLIGENT TRANSPORTATION SOCIETY OF AMERICA, Report (July13, 2001), 29 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, CC Docket 96-115 and 96-149, FEDERAL COMMUNICATION COMMISSION, Clarification order and second further notice of proposed rulemaking (September 7, 2001), 14 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, CC Docket 96-115 and 96-149, EPIC and other, Reply Comments (November 16, 2001), 9 pages.

Before the Federal Communications Commission, Washington D.C., In the Matter of the Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, CC Docket 96-115 and 96-149, THE ATTORNEYS GENERAL OF ALASKA, ARIZONA, AND MANY OTHER U.S. STATES, Comments (December 21, 2001), 13 pages.

Kanitz v. *Rogers Cable Inc.*, Docket 01-CV-214404CP, Ontario Superior Court (February 22, 2002).

3- Legal, Business, Technical Literature and Official Documents

ARC Group, *Mobile Advertising Survey – Top Level Results*, July 2001.

ARC Group, *Content and Applications for the Wireless Internet*, Worldwide Market Analysis & Strategic Outlook 2001-2006, 2001 Edition.

AT&T Wireless, *AT&T Wireless Privacy Policy*, Effective February 7, 2002. http://www.attws.com/ privacy/ (Last accessed on July 8, 2002)

Advertising Association, *Position Paper on Implementation of Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector*, United Kingdom, June 2, 1998. http://www.adassoc.org.uk/position/telcom.html (Last accessed on July 8, 2002)

Agre, Philip E., *Beyond the Mirror World: Privacy and the Representational Practices of Computing*, Technology and Privacy: The New Landscape, Eds. Philip E. Agre & Marc Rotenberg, MIT Press, 1998.

Arrison, Sonia, *Consumer Privacy: A Free Choice Approach*, PACIFIC RESEARCH INSTITUTE, September 2001. http://www.pacificresearch.org/issues/tech/privacy/privacy_home.html (Last accessed on September 15, 2001)

Bainbridge, David & Graham Pearce, *Has the New Data Protection Law failed to make a Significant Contribution to Rights of Privacy*, THE JOURNAL OF INFORMATION, LAW AND TECHNOLOGY, June 2000. http://elj.warwick.ac.uk/jilt/00-2/bainbridge.html (Last accessed on July 8, 2002)

Banahan, Mike, *Location Aware Services – Beware*, July 2000. http://www.gbdirect.co.uk/ouropinions/locationaware.htm (Last accessed on July 8, 2002)

Beales, Howard (Director, Bureau of Consumer Protection), *Privacy Notices and the Federal Trade Commission's 2002 Privacy Agenda,* Remarks to Federal Trade Commission, January 24, 2002. http://www.ftc.gov/speeches/other/privacynotices.htm (Last accessed on July 8, 2002)

Beinat, Euro, *Privacy and Location-based Services: Stating the policy clearly*, GEO INFORMATICS, September 2001.

Bellotti, Victoria, *Design for Privacy in Multimedia Computing and Communications Environments,* Technology and Privacy: The New Landscape, Eds. Philip E. Agre & Marc Rotenberg, MIT Press, 1998, 63.

Bennet, Colin J., Canadian Standards Association, *Implementing Privacy Codes of Practice,* PLUS 8830, Department of Political Science, University of Victoria, August 1995.

Bennet, Colin J., *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?,* Technology and Privacy: The New Landscape, Eds. Philip E. Agre & Marc Rotenberg, MIT Press, 1998, 99.

Bennet, Colin J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, CORNELL UNIVERSITY PRESS, 1992.

Bergqvist, Jens, Per Dahlberg, Henrik Fagrell & Johan Redström, *Location Awareness and Local Mobility-Exploring Proximity Awareness*, Viktoria Institute, 1999. http://www.viktoria.informatik.gu.se/~johan/abstracts/airis99.html (Last accessed on July 8, 2002)

Borking, John J. & Charles D. Raab, *Laws, PETs and Other Technologies for Privacy Protection*, JOURNAL OF INFORMATION LAW & TECHNOLOGY, February 28, 2001. http://elj.warwick.ac.uk/jilt/01-1/borking.html (Last accessed on July 8, 2002)

Bourrie, Sally Ruth, *Privacy or Profits?* Near Magazine, Vol. 1, Issue 1, May 2000, 33.

Cate, Fred H., *Privacy in the Information Age*, University of Indiana, Brookings Institution Press, (1997). http://www.law.indiana.edu/webinit/cate%5Fe%2Dcomm/cate/brooking.htm (Last accessed on July 8, 2002)

Center for Democracy & Technology (CDT), *Data Privacy - Wireless Location Information.* http://www.cdt.org/privacy/issues/location/ (Last accessed on July 8, 2002)

Center of Democracy and Technology (CDT), *Privacy Basics: Generic Principles of Fair Information Practice.* http://www.cdt.org/privacy/guide/basic/generic.html (Last accessed on July 8, 2002)

Clarke, Roger, *Person-Location and Person-Tracking: Technologies, Risks and Policy Implications*, XAMAX CONSULTANCY PTY LTD., October 1999. http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html (Last accessed on July 8, 2002)

Data Protection Working Party, *Privacy on the Internet – An integrated EU Approach to On-line Data Protection,* Working Document, Adopted on November 21, 2000.

Data Protection Working Party, *Second Annual Report*, Adopted on November 30, 1998.

Daum, Adam, *The Mobile Consumer*, GARTNER INC., Symposium ITxpo 2000, Orlando, Florida, October 2000.

Di Maio, Andrea, *New European Privacy Directive Addresses Location Data from Mobile Phones*, GARTNER INC., July 14, 2000.

Donaldson, Lufkin & Jenrette Securities Corporation, *The Global Wireless Communications Industry*, Summer 2000.

Dulany, Ken, *Pocket Power, Notepads, PDAs and Web Phones*, GARTNER INC., Symposium ITxpo 2000, Orlando, Florida, October 2000.

Egan, Bob & Peter Richardson, *Wireless Access Evolution and Economics*, GARTNER INC., Symposium ITxpo 2000, Orlando, Florida, October 2000.

Egan, Bob, *Mobile and Wireless Computing: The Next User Revolution*, GARTNER INC., Symposium ITxpo 2001, Orlando, Florida, October 2001.

Escuerdo, Alberto, Martin Hedenfalk & Per Heselius, *Flying Freedom, Location Privacy in Mobile Internetworking*, Royal Institute of Technology, Sweden, April 26, 2001.

Escuerdo, Alberto, *Anonymous and untraceable communications; Location privacy in mobile internetworking*, Laboratory of Telecommunications Systems, Royal Institute of Technology, Sweden, May 16, 2001.

European Commission, *Junk E-Mail Costs Internet Users Euro 10 Billion a Year Worldwide*, Study, February 2, 2001.

European Commission, Data protection working party - *Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act*, Adopted on January 26, 2001.

European Commission, *Draft Commission Decision on the adequacy of the protection provided by the Safe Harbor Principles and related Frequently Asked Questions issued by the US Department of Commerce*, June 5, 2000.

European Commission, *The processing of personal data and the protection of privacy in the electronic communications sector*, DG Information Society Working Document, Communications Services, Policy and Regulatory Frameworks, Brussels, April 27, 2000.

Fasbender, Andreas, Dogan Kesdogan and Olaf Kubitz, *Variable and Scalable Security: Protection of Location Information in Mobile IP*, Aachen University of Technology, IEEE VTS, 46th Vehicular Technology Conference, Atlanta, GA, April 28-May 1, 1996.

Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*, May 2000.

Federal Trade Commission, *Privacy Online: A Report to Congress,* June 1998.

Federal Trade Commission, *Public Workshop: Consumer Privacy on the Global Information Infrastructure*, Official Transcript Proceedings, Washington D.C., June 4, 1996.

Federal Trade Commission, *Public Workshop: Consumer Privacy on the Global Information Infrastructure*, Official Transcript Proceedings, Washington D.C., June 5, 1996.

Federal Trade Commission, *Public Workshop: Consumer Privacy on the Global Information Infrastructure*, Staff Report, December 1996.

Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, Washington D.C., March 13, 2001. http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm (Last accessed on April 15, 2001)

Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging technologies and Consumer Issues*, December 11-12, 2000. http://www.ftc.gov/opa/2000/11/wireless.htm (Last accessed on July 8, 2002)

Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 11, 2000. http://www.ftc.gov/bcp/workshops/wireless/001211.htm (Last accessed on July 8, 2002)

Federal Trade Commission, *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, Wireless Web Workshop, December 12, 2000. http://www.ftc.gov/bcp/workshops/wireless/001212.htm (Last accessed on July 8, 2002)

Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress*, July 1999.

Federrath, Hannes, Anja Jerichow & Andreas Pfitzmann, *MIXes in Mobile Communications Systems: Location Management with Privacy*, University of Dresden, Institute of Theoretical Computer Science, D-011062, Dresden, Germany, June 1996.

Fenn, J., *Mr. President, Get ready for a Wireless, Wearable World*, GARTNER INC., Research Note., March 20, 2001.

Gartner Inc., *Will SMS Be the Catalyst of a Global Messaging Revolution?,* Research Brief, February 19, 2001.

Gassman, Bill & Arabella Hallawell, *Aggregate Data Will Become the Next Privacy Battleground*, GARTNER INC., FirstTake, FT-13-2000, February 7, 2001.

Gauthronet, Serge & Étienne Drouard, *Unsolicited Commercial Communications and Data Protection – Summary of Study Findings*, Commission of the European Communities, Internal Market DG – Contract no ETD/99/B5-3000/E/96, January 2001.

Gellman, Robert, *Does Privacy Law Work?* Technology and Privacy: The New Landscape, Eds. Philip E. Agre & Marc Rotenberg, MIT Press, 1998. 193.

Gidari, Albert, *Location Privacy: Fair Location Information Practices for Mobile Commerce*, Prepared for Location Decisions 2000 – Application of Location Technology for the International Commercial Environment, Chicago, Illinois, June 13-14, 2000.

Girard, John & Roni Colville, *Mobile Device Management and Synchronization: Take Control or Lose Control*, GARTNER INC., Symposium ITxpo 2001, Orlando, Florida, October 2001.

Girard, John & John Pescatore, *Security on the Run: Mobile and Wireless Security*, GARTNER INC., Symposium ITxpo 2001, Orlando, Florida, October 2001.

Goldman Sachs, *Technology: Mobile Internet*, MOBILE INTERNET PRIMER, July 14, 2000.

Gurski, Mike & Ann Cavoukian, *Privacy in the Wireless World*, Ontario Information and Privacy Commission, July 25, 2001.

Hallawell, Arabella, *Mr. President, It's time* for New Privacy Protection methods, GARTNER INC., Research Note, March 1, 2001.

Hallawell, Arabella, *Beyond the Headlines: Privacy Issues and the Enterprise*, GARTNER INC., May 4, 2001

Hamilton, Elliot, *Wireless location Marketplace*, Presentation at the WLIA Wireless Location Industry Issues Workshop, THE STRATEGIS GROUP INC., January 31, 2001.

Hendricks, Evan, *Wireless location Technology: The Ultimate Challenge to Privacy*, Before the XXIII International Conference Of Data Protection Commissioners, September 24, 2001.

Hes, R. & J. Borking, *Privacy-enhancing technologies: the path to anonymity,* Revised edition, Registratiekamer, in cooperation with the Ontario Information and Privacy Commissioner, Achtergrondstudies en Verkenningen 11, The Hague, November 1998. http://www.registratiekamer.nl (Last accessed on July 15, 2001)

Industry Canada, Stratégie canadienne, *Le commerce électronique au Canada – Vie privée: Protection des renseignements personnels*, Groupe de travail sur le commerce électronique, 1998. http://e-com.ic.qc.ca/francais/privee/632d21.html (Last accessed on July 15, 2001)

Industry Canada, Le commerce électronique au Canada: Instaurer la confiance dans l'économie numérique, *Sécurité et cryptographie – Politique cadre en matière de cryptographie aux fins du commerce électronique*, Pour une économie et une société de l'information au Canada, December 10, 2000. http://e-com.ic.gc.ca/francais/crypto/631d13.html (Last accessed on July 8, 2002)

INSEAD, *The New Wireless Economy*, An independent Analysis of the Competitive Forces, Revenue Models and Wireless Advertising Possibilities, 2001.

Intelligent Transportation Society of America, *ITS America's Intelligent Transportation Systems – Fair Information and Privacy Principles*, December 13, 1994, 3 pages.

ITS America, *Briefing to Wireless Location Industry Association*, ITS America Activities, Presentation at the WLIA Wireless Location Industry Issues Workshop, January 31, 2001.

Jones, Nick, *Mobile E-Business Scenario*, GARTNER INC., Symposium ITxpo 2000, Orlando, Florida, October 2000.

Jones, Nick, *Mobile Commerce Business Scenario*, GARTNER INC., Symposium ITxpo 2001, Orlando, Florida, October 2001.

Karn, Phil, *Cell Phone Tracking*, Essay on Cellular Phone Tracking, 1997. http://people.qualcomm.com/karn/papers/index.html (Last accessed on July 17, 2002)

Kelsey Group (The), *Voice & Wireless Commerce*, Document VWC-WP0102, 2001.

Kobb, Bennett, *Consumer Convenience and Emergency Assistance or Privacy Invasion*, Civil Rights Forum on Communication Policy, The Forum Connection, September 2001. http://www.civilrightsforum.org/tech092001.html (Last accessed on July 17, 2002)

Levijoki, Sami, *Privacy vs Location Awareness*, Helsinki University of Technology, Department of Computer Science, 2000. http://www.hut.fi/~slevijok/privacy_vs_locationawareness.htm (Last accessed on July 8, 2002)

Location Inter-operability Forum (LIF), *LIF Statement*, Version 5, March 14, 2001. http://www.locationforum.org/ (Last accessed on July 8, 2002)

Mabley, Kevin, *Privacy vs. Personalization – Personalization: A threat to privacy?*, CYBER DIALOGUE INC., 2000.

Mbusiness, Voice of the Mobile Economy, *M-Services: Promises, Promises*, June 2001, 60.

Mbusiness, Voice of the Mobile Economy, *Personalization's wireless potential*, June 2001, 73.

McGuire, Mike, *Mobile Business Markets: What Can't Users Live Without*, GARTNER INC., Symposium ITxpo 2001, Orlando, Florida, October 2001.

Miller, Gregory A., *In re The Mobile Wireless Web, Data services and beyond: Emerging technology and consumer issues, A Public Workshop – Response Statement for Day II panel: Building Privacy and Security Solutions into the Technological Architecture*, December 11, 2000. http://www.ftc. gov/workshops/wireless/comments/miller.htm (Last accessed on July 30, 2001)

Mobile Lifestreams, *Yes 2 SMS – Short Message Service Opportunities*, April 1, 2000.

Mobile Lifestreams, *Success 4 WAP*, White paper, February 2001.

Mobile Marketing Association, *Wireless Advertising Trials Research*, September 20, 2000.

Mobilocity.net, *Seizing the M-Commerce Opportunity – Strategies for Success on the Mobile Internet*, White paper, May 2000.

Muris, Timothy J., Chairman of the FTC, *Protecting Consumers' Privacy: 2002 and Beyond*, The Privacy 2001 Conference, Cleveland, Ohio, October 4, 2001. http://www.ftc.gov/speeches/muris/privisp1002.htm (Last accessed on July 8, 2002)

Nelson, Rosalie, *Mobile Advertising: Building Alternative Revenue Streams*, OVUM, Short Report 20, June 2000.

Nelson, Rosalie & Neil Ward-Dutton, *Wireless Marketing: Rhetoric, Reality & Revenues*, OVUM, Report, June 2001.

Nokia Inc., *Contextual Demand for Value-Added Services*, Market Study for VAS, June 2000.

Online Privacy Alliance (OPA), *"Online Consumer Privacy in the United States" Submitted with the Comments of the Online Privacy Alliance, On the Draft International Safe Harbor Principles*, White Paper, November 19, 1998. http://privacyalliance.org/news/12031998-5.shtml (Last accessed on July 8, 2002)

Ozanich, Gary W., *The Wireless Marketing Opportunity,* THE KELSEY GROUP, April 10, 2001.

PriceWaterHouse Coopers, *Technology Forecast: 2001-2003 – Mobile Internet: Unleashing the Power of Wireless*, April 2001.

Privacy Commissionner of Canada, *Findings regarding complaints about Air Canada's Aeroplan Frequent Flyer Program under the Personal Information Protection and Electronic Documents Act*, New release, Ottawa, March 20, 2002. http://www.privcom.gc.ca/media/nr-c/02_05_b_020320_e.asp (Last accessed July 8, 2002)

Profilium Inc., *Platform for Predictive Services*, Business Plan, Montreal, Canada, 2000.

Quios and Engage, *The Efficacy of Wireless Advertising*, Industry Overview and Case Study, 2000.

Reynolds, Martin, *Wireless Location Services: Who's watching You?*, GARTNER INC. May 9, 2001. http://www3.gartner.com/DisplayDocument?id=329970&acsFlg=accessBought (Last accessed on July 8, 2002)

Rotenberg, Marc, *Technology and Privacy: The New Lanscape*, Electronic Privacy Information Center, MIT Press, 1997. http://dlis.gseis.ucia.edeu/people/pagre/lanscape.htm (Last accessed on July 15, 2001)

Schmidt, Carsten, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001.

Schwartz, Ari & Alan Davidson, *Location, Location, Location: The Emerging Crisis in Wireless Data Privacy*, Center for Democracy and Technology, Power point presentation, 2001. http://www.cdt.org (Last accessed on July 15, 2001)

Stanley, Jay, *Wireless Ushering In A New Phase In Privacy Wars*, THE FORRESTER BRIEF, December 21, 2000.

Strategis Group, *Wireless Location Services: 1999,* October 20, 1999.

Surtees, Lawrence, *Never Lost, Always Found: The business case for privacy*, IDC Canada, 2nd Annual Privacy and Security Workshop, Faculty Club, University of Toronto, November 1, 2001.

Surtees, Lawrence, *Nowhere to Hide: Privacy Implications of Wireless Location Technology*, IDC Canada Bulletin, Canadian Telecom Market Drivers and Strategies, March 2001.

Syverson, Paul F., David M. Goldschlag & Michael G. Reed, *Protocols using Anonymous Connections: Mobile Applications*, Naval Research Laboratory, 1998.

Swire, Peter, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, Draft submitted to NTIA, December 23, 1996. http://www.osu.edu/units/laws/swire1/psntia6.htm (Last accessed on July 15, 2001)

UMTS Forum, *Enabling UMTS/Third Generation Services and Applications*, Report No. 11, October 2000.

UMTS Forum, *The UMTS Third Generation Market – Structuring the Service Revenues Opportunities*, Report No. 9, September 2000.

Waryas, Keith, Callie Nelsen & Kevin Burden, *Ten Key Trends in Mobile eBusiness*, IDC, 2001.

Windwire Inc., *First-to-Wireless: Capabilities and Benefits of Wireless Marketing and Advertising Based on the First National Mobile Marketing Trial*, December 27, 2000.

Wireless Location Industry Association, *WLIA's Process to Achieve Self-Regulation to Protect Wireless Device User's Privacy Rights in Signal Location Applications*, 2001. http://www.wliaonline.org/ (Last accessed on July 15, 2001)

Wireless Location Industry Association, *FCC Seeks New Comments on Customer Consent for Use of Customer Proprietary Network Information (CPNI), Including Location Data*, Newsletter, October 12, 2001. http://www.wliaonline.com/publications/fcccpni.html (Last accessed on July 8, 2002)

Zimran, Ahmed & Mark Hurst, *The Wireless Customer Experience – An Introduction*, CREATIVE GOOD, September 2000.

4- News Articles and Press Releases

AllNetDevices, *Privacy Not Major M-Commerce Issue, Study*, October 15, 2001. http://www.allnetdevices.com/wireless/news/2001/10/15/privacy_not.html (Last accessed on July 17, 2002)

AllNetDevices, *Location Privacy Bill Introduced*, July 13, 2001. http://www.allnetdevices.com/icom_cgi/print/print.cgi?url=http://www.allnetdevices.com/wireless/news/2001/07/13/location_privacy.html (Last accessed on July 17, 2002)

AllNetDevices, *Location Services Coming Slowly*, July 12, 2001. http://www.allnetdevices.com/icom_cgi/print/print.cgi?url=http://www.allnetdevices.com/wireless/news/2001/02/15/ revenue_forecasts.html (Last accessed on July 17, 2002)

American Bankers' Association, *ABA Survey Shows Nearly One Out of Three Consumers Read Their Banks Privacy Notices*, Press release, June 15, 2001. http://www.aba.com/Press+Room/bankfee060701.htm (Last accessed on July 8, 2002)

Anywhereyougo.com, *L-Commerce 2001 Offers Strategies to Monetize Location-Based Services*, April 23, 2001. http://www.AnywhereYouGo.com/wireless/Article.po?id=405191 (Last accessed on July 8, 2002)

Black, Jane, *What Price Privacy? - Companies Should Stop Wielding Scary Numbers and Help Design a Law that Will Protect Consumers -- and Make Business More Efficient,* BUSINESS WEEK ONLINE, June 7, 2001. http://www.businessweek.com/bwdaily/dnflash/jun2001/nf2001067_517.htm (Last accessed on July 8, 2002)

Borland, John, *Wireless Phone Tracking Plans Raise Privacy Hackles*, CNET, NEWS.COM, November 10, 2000. http://news.cnet.com/news/0-1004-200-3624256.html (Last accessed on July 8, 2002)

Brewin, Bob, *Digital Angel to Watch Over Patients - but Some Fear System Could Be Big Brother*, COMPUTERWORLD, January 1, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47STO55670,00.html (Last accessed on July 8, 2002)

Cnetnews.com, *Secure Mobile Phones Come to Market*, June 4, 2001. http://investor.cnet.com/investor/news/newsitem/0-9900-1028-6186906-0.html (Last accessed on July 17, 2002)

Cnn.com, *Internet Devices Coming that Reveal your Location*, October 30, 2000. http://www.cnn.com/2000/TECH/computing/10/30/wireless.tracking.ap/ (Last accessed on July 8, 2002)

Crouch, Cameron, *Will Big Brother Track You by Cell Phone?*, CNN.COM, April 20, 2001. http://www.cnn.com/2001/TECH/ptech/04/20/location.services.idg/index.html (Last accessed on July 8, 2002)

Diercks, Rebecca, *Mobile Advertising: Not as Bad as You Think - Early Adopters Indicate Reluctance, but May Warm to Discounts – with Choice and Privacy*, WIRELESS INTERNET MAGAZINE, Cahners In-Stat Group, July/August 2001. http://www.wirelessinternetmagazine.com/news/0108/0108_research_ads.htm (Last accessed on July 8, 2002)

Emarketer.com, *US Wireless Firms Choose Opt-In to Protect Privacy*, June 6, 2001. http://www.emarketer.com/estatnews/enews/reuters/06_05_2001.rwntz-story-bcnettechprivacywirelessdc.html (Last accessed on June 6, 2001)

European Union, *Proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sec*tor, Bulletin EU 11-2001, Information Society 7/11, November 13, 2001. http://europa.eu.int/abc/doc/off/bull/en/200111/p103104.htm (Last accessed on July 8, 2002)

Glasner, Joanna, *Feds OK Cell Phone Tracking*, WIRED NEWS, September 16, 1999. http://www.wired.com/news/topstories/0,1287,21781,00.html (Last accessed on July 8, 2002)

Hamblen, Matt, *Ensuring Portable Privacy - Banks, Retailers and Airlines Face the "Opt-In" Issue and Other Challenges*, COMPUTERWORLD, December 11, 2000. http://www.computerworld.com/cwi/story/ 0,1199,NAV47_STO54794,00.html (Last accessed on July 8, 2002)

Hamblen, Matt, *Location Information Could Invade Privacy of Wireless Users, Analysts Warn*, COMPUTERWORLD, September 28, 2000. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO51388,00.html (Last accessed on July 8, 2002)

Hamblen, Matt, *Privacy Concerns Mount over Wireless Location Technology*, COMPUTERWORLD, February 13, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57662,00.html (Last accessed on July 8, 2002)

Hamblen, Matt & Bob Brewin, *Need to Find a Customer,* COMPUTERWORLD, April 16, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59621,00.html (Last accessed on July 8, 2002)

Haskin, David, *Wireless Advertising: Will Anybody Ever Care?,* ALLNETDEVICES, May 7, 2001. http://www.allnetdevices.com/industry/reality/2001/05/07/wireless_advertising.html (Last accessed on July 8, 2002)

Industry Canada, *European Commission Recognizes Canadian Legislated Privacy Protection,* Ottawa, January 14, 2002.

Khan, Basheera, *Mobile Marketing Takes SMS into the Future*, IT WEB–the technology website, September 17, 2001. http://www.itweb.co.za/sections/quickprint/print.asp?StoryID=114578 (Last accessed on July 15, 2001)

Kotch, Micah, *Maximizing Mobile Marketing Opportunities*, CLICKZ REPORT, October 5, 2001. http://www.clickz.com/wireless/ad_comm/article.php/897831 (Last accessed on July 8, 2002)

Mobile Marketing Association, *WAA and WMA Merge to Expand Global Forum for Standards in Mobile Marketing - Leading Industry Bodies Join Forces to Set Standards and Deliver New Benefits for Member,* Press Release, January 10, 2002. http://www.waaglobal.org/press/merger1-10_press.shtml (Last accessed on July 8, 2002)

Oakes, Chris, *Zeroing In on Cell-Phone 911s*, WIRED NEWS, June 30, 1999. http://www.wired.com/news/technology/0,1282,20504,00.html (Last accessed on July 8, 2002)

Romero, Simon, *Location Devices Gain in Popularity but Raise Privacy Concerns,* N.Y. TIMES, March 4, 2001. http://www.nytimes.com/2001/03/04/technology/04LOCA.html (Last accessed on March 4, 2001)

Ross, Patrick, *Bill Aims to Block Wireless Junk Email,* CNET NEWS.COM, January 10, 2001. http://news.cnet.com/news/0-1004-200-4432707.html (Last accessed on January 10, 2001)

SignalSoft, *SignalSoft's New Access Manager™ Provides Mobile Subscribers with Enhanced Privacy and Authentication Capabilities*, June 19, 2001. http://www.signalsoftcorp.com/newsroom/pressreleases/q2_2001/press_sgsfam.html (Last accessed on July 8, 2002)

Silk, Jon, *Brand New Message SMS Marketing Finds its Voice*, M-COMMERCE WORLD.COM, September 28, 2001. http://www.mcommerceworld.com/articles/article.cfm/952E7614-A21E-403B-A8AD8214DE36DE49 (Last accessed on September 28, 2001)

United States Senate, *Senator Edwards Proposes Location Privacy Law*, North Carolina, Press Release, July 11, 2002. http://edwards.senate.gov/press/2001/jul11-pr.html (Last accessed on July 8, 2002)

Wayner, Peter, *Technology that Tracks Cell Phones Draws Fire*, N. Y. TIMES, February 23, 1998). http://www.nytimes.com/library/tech/98/02/biztech/articles/022398track.html (Last accessed on July 8, 2002)

Wireless Location Industry Association, *FCC Seeks New Comments on Customer Consent for Use of Customer Proprietary Network Information (CPNI), including Location Data*, Newsletter, October 12, 2001. http://www.wliaonline.com/publications/fcccpni.html (Last accessed on July 8, 2002)

Wireless Location Industry Association, *WLIA Wireless Location Industry Issues Workshop Wednesday, January 31, 2001 Washington, DC.*, NEAR MAGAZINE, Newsletter, March 2001. http://www.wliaonline.org/publications/wliaworkshop.html (Last accessed on July 8, 2002)

Wrostad, Jay, *Where's the Fire? E911 Strategies Slow To Ignite*, WIRELESS NEWSFACTOR, June 7, 2001. http://www.wirelessnewsfactor.com/perl/story/10091.html (Last accessed on July 8, 2002)