M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising

Eloïse Gratton †

Introduction

Mobile commerce ("m-commerce") has been defined as the facilitation of monetary transactions, including the purchase of products or services, using wireless devices, like digital wireless phones or a personal digital assistant (PDA), to access the Internet using a wireless data connection or a private network.[1] As evidenced by the smashing success of companies like NTT DoCoMo,[2] m-commerce represents a significant opportunity for companies to increase revenues, improve customer service and build their brand. However, according to a report from Goldman Sachs[3] on the mobile Internet, in order to capitalize on the m-commerce opportunity, companies need to consider m-commerce as highly personalized, easy-to-use, transaction-oriented, and location-specific.[4]

In order to provide wireless users with content or advertising that is personalized and location-specific, service providers may use the location data of the wireless user's device derived from pinpoint tracking technologies that are either network-based solutions (relying on accessing information in a carrier's home location register to locate the wireless device) or handset-based solutions that rely on a global positioning system ("GPS") where information derived from a GPS chip in the wireless device is reported to the provider over the wireless network.

Using these pinpoint tracking technologies, m-commerce can potentially create and target advertising messages and campaigns 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 and advertising analysis tool for businesses.[5] It could also enable them to customize and personalize advertising for wireless users.

The development of location-based advertising, 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 an 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. Wireless users would receive unanticipated advertising messages on their wireless device, commonly referred to as "wireless spam", generally considered a form of privacy violation.

Even if North American and Europeans laws, regulations and directives related to the protection of personal data and against the proliferation of unsolicited messages seem to be providing a general legal framework for a company wishing to provide a new service such as location-based advertising (the "service provider"), these rules are in some cases vague, and are not specific to this new context. More specifically, these regulations do not specify what should constitute an appropriate and effective disclosure in order to obtain meaningful consent from the wireless user agreeing to receive such messages. For example, would the wireless users actually know that, when consenting to advertising, they are also agreeing to being tracked and having their location data collected and stored by a third party?

In order to obtain a valid consent from the wireless user, the service provider will have to make an effective disclosure that covers all of the tracking- and storage-related issues. Also, an analysis of the present laws, regulations and directives, as well as the specific nature of this type of service, may help determine what aspects the consent of the wireless user should cover in order to protect the user from receiving wireless spam.

This paper is, therefore, meant to propose a solution, demonstrating how a service provider may obtain informed and meaningful consent from the wireless users prior to providing them with location-based advertising. Consent would also comply with the different laws and regulations regarding the protection of personal and location data as well as spam control.

†LL.M. (Information Technology Law), 2002, University of Montreal. Member, Barreau du Québec. Associate, Mendelsohn Law firm.

Location-Based Advertising

Location-based advertising allows wireless users to receive content relative to their geographic position and based on the fact that their needs may vary depending on where they are and when they are using their devices.[6] Wireless marketing consists of the delivery of advertisements, coupons and other forms of promotional and transaction-driven content to wireless devices.[7] It has been defined as "total activities involved in communicating to a mobile audience through the use of untethered devices with the goal of increasing awareness, disseminating information, and promoting the sale of goods or services".[8] These messages may be delivered to multiple devices: WAP phones, PDAs, two-way pagers and SMS-enabled devices. Using the medium for sales and promotion alerts that give wireless users 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.

Location specific advertising and personalization in the wireless world are achieved through the use of location data gathered by tracking technology and, more specifically, the use of historical location data and real-time location data. There are two main kinds of tracking technologies now available on the market in order to gather location data that carriers in the United States are presently deploying. This follows 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. The first method includes network solutions that use two cellular towers to describe the interconnection of signals with a user, which is the technology used by carriers like Verizon Wireless[9] and Western Wireless.[10] The second type of tracking technology is the handset-based solution, which includes GPS phones, the technology used by carriers such as Sprint PCS,[11] Alltel[12] and Nextel[13] favouring handsets equipped with GPS chips.[14]

Personalization

According to the Personalization Consortium,[15] personalization is the use of technology and customer information to tailor interactions between a business and individual customers to fit that customer's stated or perceived needs, in order to make the interaction efficient and satisfying for both parties and build a relationship that encourages loyalty. Forrester Research[16] is suggesting that in the same way as the ad networks such as DoubleClick[17] and Engage[18] are doing today, the best content providers will understand the behavioural patterns of the wireless users and will deliver context-relevant advertising or content, which would make wireless users more accepting of location-based advertising, according to a study done by Quios[19] and Engage[20] on the efficiency of wireless advertising.[21]

The flipside of personalization is, as outlined by the Center for Democracy and Technology[22] ("CDT"), the fact that profiling can be threatening and consumers have already grown weary of such practices.[23] As a matter of fact, personalization on the Internet has been criticized. 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.[24]

In order to make the advertising message accurately personalized to each wireless user in a timely manner, many advertisers may utilize a combination of static demographic and psychographic data ("Static Profile"), with location data that is collected over time and based on the wireless user's habits, lifestyle, preferences, and location patterns ("Dynamic Profile").

Static profiling: Demographic and psychographic data

One way to make personalization work in the wireless world is to place consumers in charge of this process, as mentioned by Evan Hendricks from Privacy Times.[25] He had the opinion that the involvement of the wireless user will play a big role in the short run and that a lot of m-commerce applications will be based on the profiles provided by participants.[26] For example, a wireless user interested in receiving location-based advertising may voluntarily provide information regarding his/her gender, age, interests, etc., to the service provider in order to receive personalized content based on this Static Profile. As a matter of fact, companies wishing to provide location-based advertising should obtain personal information from the participant.[27]

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 ("Dynamic Profiling"), especially since a wireless device is time sensitive and typically used by only one individual[28] which allows it to "push" content based on the user's unique profile.

This type of profiling is possible today mainly for carriers or service providers using network-based tracking technology, as opposed to handset tracking technology,[29] since they are using one that 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, even in the 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 advertising. 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.[30]

Location specific: Real time location data

Location data may provide the means to use real-time positioning as a trigger for marketing messages. 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 the advertising message relevant.

Privacy Issues

A critical aspect of successful location-based advertising lies in understanding the potential for the intrusiveness of the medium, since most wireless users carry their wireless phones round the clock, as well as respecting the need for the consumer's rights to decline receiving such messages.

The privacy issues surrounding location-based advertising and facing wireless users can be separated into two main categories. The first issue is related to tracking, where the problem is that, over time, historical location data collected and stored in databases — that may enable advertisers to deliver very helpful, location-specific information to wireless users — will also enable a service provider to build a very detailed and invasive dossier of a wireless user's travel patterns, movements and other habits. The second issue is related to the real-time location data that would be used to send advertising messages to the wireless user supposedly at the right place to make the message relevant, which could be very intrusive if such advertising is unanticipated by the user.

Windwire[31] 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. Their report, published in December 2000, states that, according to their study, 64% of participants were concerned with privacy issues and "push" location-based advertising in particular.[32]

The uncontrolled availability of location data, and the possibility of wireless spam, present serious risks to individual privacy. In his report, entitled "Privacy in the Wireless World",[33] Mike Gurski, Senior Technology Advisor for the Ontario Information and Privacy Commission, raises one of the most problematic privacy issues facing the wireless world — the notion of "meaningful consent" related to a location-based service such as advertising:

> 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 be meaningful, however, it must be *informed*. This is becoming increasingly difficult as technology outstrips the guidelines that govern it.[34]

As a matter of fact, there are many privacy issues surrounding the notions of "disclosure" and "consent" specific to location-based advertising that are not clearly addressed in the current privacy laws and regulations in order to adequately protect the privacy of wireless users.

Disclosure

Disclosure (also known as "notice" or "privacy policy") is the most fundamental of all principles. Without appropriate and effective disclosure, a wireless user cannot make an informed decision as to what extent to disclose personal information, if at all, or to agree to being tracked, and whether the user wishes to receive location-based advertising. In the specific context of location-based advertising, disclosure is the notice to the wireless user of the tracking and the collection of his/her personal or location data that will take place, regardless of whether messages will be sent to such user.

At the same time, in today's wireless communications networks, location data giving the geographic position of wireless users, or strictly speaking that of their terminal equipment, already exists. This information is necessary to enable the transmission of communications to and from a user without a fixed location. Current wireless device networks can locate a user based on the closest cell phone tower, to within a distance ranging from several hundred feet to several miles.[35] For this reason, it is not clear if it would be appropriate to even disclose to the wireless user that s/he will be tracked, considering the fact that today the network already knows where the user is.

Legal framework related to disclosure

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 an 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 ("PII"), which 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, and e-mail address.[36] Since these laws and regulations were put in place to protect the personal information of consumers, they may not apply when anonymous location data is stored and used by third parties, since the purpose is no longer applicable. However, in many cases, since location data contains PII, or there is a threat that location data will be merged with PII, or personal information will be available through the storage of such data, this paper will

present an analysis of both the regulations regarding the protection of personal data and the attempts to regulate the protection of location data.

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[37] are explicit to the effect that the purposes for which personal data is collected should be specified no later than at the time of data collection.[38] These guidelines also state that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means of establishing the existence and nature of personal data and the main purposes of their use should be readily available, as well as the identity and usual residence of the data controller.[39]

In Europe, Directive 95/46/EC[40] states that personal data must be processed fairly and lawfully collected for specified, explicit and legitimate purposes and should not be further processed in a way to be incompatible with those purposes.[41] On July 12, 2000, the European Commission issued a proposed directive for an amendment to the Data Privacy Directive,[42] in order to update provisions to cope with the evolution of technology, such as the move from fixed to wireless communications and from voice to data, which proposal was accepted in November 2001 by the European Parliament.[43] The proposal introduces safeguards for wireless users with regards to mobile location information services.[44] It gives users the right to refuse unsolicited communications for direct marketing purposes and extends coverage to all forms of electronic communications.[45]

In North America, the United States' Safe Harbor Agreement[46] went into effect on November 1, 2000, and 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 to adequately meet the European Union's data privacy Directive, which is 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, the purposes for which it collects such information, the type of organizations to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.[47] 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.[48]

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. The *Wireless Privacy Protection Act of 2001*[49] was introduced in the House of Representatives on January 30, 2001, by Mr. Frelinghuysen. It requires that the individuals 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 the individual originally disclosed it.[50] Also, a customer shall not be considered to have granted express prior authorization unless the carrier has provided in writing to the customer a clear, conspicuous, and complete disclosure of the carrier's practices with respect to the collection and use of location information, before any such information is disclosed or used. Such disclosure includes a description of the specific types of information that is collected by the carrier[51] and how the carrier uses such information.[52] Also, the *Location Privacy Protection Act of 2001*[53] was introduced into the U.S. Senate in July 2001 in order to protect the privacy of users of wireless devices that pinpoint their location. The bill states that the providers of location-based services and applications have to inform customers, with clear and conspicuous notice, about their policies on the collection, use, disclosure, retention, and access to customer location information.[54]

In Canada, the *Personal Information Protection and Electronic Documents Act*[55] 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 standard CSA Model Code for the Protection of Personal Information, which has the potential to operate in the same way as many other quality-assurance standards such as the increasingly popular ISO 9000 series.[56] The Act, which initially only applied to federally regulated companies as of January 2001, by the year 2004 will extend its application to every organization that collects, uses or discloses personal information in the course of a commercial activity. This will apply whether or not the organization is a federally-regulated business, so that an organization may only collect, use or disclose personal information for purposes that a reasonable person would consider are appropriate under the circumstances[57] and with the knowledge or consent of such an individual.[58]

The Act states that the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.[59] Depending upon the way in which the information is collected, the law mentions that this disclosure could be done orally or in writing,[60] for example, through an application form.[61] In accordance with such law, an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information[62] including (i) the name, title, and address of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;[63] (ii) the means of gaining access to personal information held by the organization;[64] (iii) a description of the type of personal information held by the organization, including a general account of its use;[65]

(iv) copies of any brochures or other information that explain the organization's policies, standards, or codes;[66] and (v) what personal information is made available to related organizations including subsidiaries.[67] The Act further suggests that an organization may make information on its policies and practices available in a variety of ways depending on the nature of its business and other considerations. It may also choose to make brochures available in its place of business, to mail information to its customers, to provide online access, or to establish a toll-free telephone number.[68]

Practical issues related to disclosure

Even if these laws and regulations provide, in a general way, the legal framework to enable service providers to disclose the purpose of the location data collection prior to such collection or use of the data, the complete details surrounding disclosure to ensure that it is effective in the context of location-based advertising have never been addressed or 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 disclosure in the context of providing location-based advertising follows.

Who should be provided with disclosure?

In a general way, the North American and European laws and regulations, analyzed above, mention that disclosure should be made to the subject prior to data collection. These laws do not specify whether the tracking should be disclosed only to the users who have agreed to receive advertising 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.

On this last issue, there seems to be a different status for anonymous tracking. For example, Nextel Communications Inc.[69] points out the fact that there should be a distinction made for wireless users tracked anonymously and that the statutory requirements for customer "express prior authorization" and the foregoing location data 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 aggregate customer information which is not personally identifiable.[70]

Who should be responsible for providing disclosure?

The laws and regulations analyzed above mention that the data collector should make the disclosure, without specifying if, in the case of location-based advertising, we are referring to the actual location data collector or the user of such data. As a matter of fact, one of the main issues related to disclosure is determining which party should be in charge of providing the disclosure relating to the tracking of the wireless users. Should it be the service provider that actually deploys the location-based advertising service, 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.

Each of the CDT[71] and Fiderus Strategic Security and Privacy Services[72] shares the views that each party involved in providing this type of location-based advertising service should be involved in assuring the wireless user that the collected data is protected.[73] The position that the disclosure should come from all of the parties may not be a very practical one, given that it may require too much coordination between the wireless device manufacturer, the carrier, the service provider, and the advertiser and would more than likely only further confuse the wireless user.

How should the disclosure be given?

One unique problem for disclosure is the fact that a wireless device — in contrast to a desktop computer — has unique characteristics that include a relatively small screen size limiting the ability of carriers or service providers to display a privacy notice or a disclosure directly on the hand-held device. The laws and regulations analyzed above never specify how the disclosure should be made in the context of location-based advertising services. Also, the legal framework does not specify if such disclosure should be oral or in writing and more specifically, how a service provider can possibly make an effective disclosure on the small screen of a wireless device.

There may be a better way for service providers to make their disclosure rather than on the wireless device screen, especially since most of the wireless phones on the market only have a capability of containing 160 characters. But what is the appropriate way? Wireless Consumers Alliance Inc.[74] states that a disclosure would not be considered appropriate if buried in other documents or letters or if the wireless users have to undertake steps to learn of the invasion of their privacy.[75]

When should disclosure be given?

When disclosure should be given to the wireless user is an important issue. The present laws do not seem to agree on when disclosure should take place: some laws state that disclosure takes place prior to the collection of data,[76] while others state that it takes place prior to the use of such collected data.[77]

The Cellular Telecommunications and Internet Association[78] ("CTIA"), the main trade association for wireless companies in the United States, petitioned the FCC in November 2000 to begin a rule-making procedure for tracking the location of wireless users (the "Peti-

tion"). It seems to agree with the position that service providers should inform the wireless user about the specific location of data collection[79] and use practices before any use of the location data takes place.[80] On a more practical point of view, it should be determined if, for example, disclosure should be provided when a phone is sold or later, perhaps over a desktop computer hooked up to the Internet.

What should be the content of disclosure?

In a general way, the laws and regulations analyzed above, with regards to the content of disclosure, may specify certain information that needs to be disclosed, while omitting to mention other important relevant information. For example, none of the laws analyzed were complete regarding information that should be covered in an effective disclosure, including whether the wireless user should simply be informed when location data is collected or why tracking is 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 Web site.[81] The policy, if only analyzed in the context of providing location-based advertising, would not be sufficient. For example, the 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.[82]

The Ontario Superior Court of Justice has recently ruled in *Kanitz v. Rogers Cable Inc.*[83] that such procedure of notifying changes to a privacy policy via web posting was adequate. 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/her 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.

Choice and Consent

There are many privacy issues related to consent including "how choice should be provided and who should provide it"[84] in the context of location-based advertising.

First to consider is the consent by the wireless user to being tracked. Within this issue, there is a distinction to be made between users that are being tracked for the purpose of being provided with push location-based advertising, users that are being tracked with the knowledge from a third party collecting identity data, and users that are being tracked anonymously.

Second, consent may have to be given not only prior to the tracking of the wireless user, but also prior to sending advertising messages to the user on a "push" basis. Such procedure would avoid spam-related issues. Also, this last form of consent implies many other things, including the type, location and frequency of received advertising messages to which a wireless user may agree.

Legal framework

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.

Regulations related to the collection or use of personal and location data

According to the OECD Guidelines[85] where appropriate, the collection of personal data and any such data should be obtained with the knowledge or consent of the data subject[86] and 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.[87]

In Europe, the EC Directives[88] state that personal data may be processed only if the data subject has unambiguously given his/her consent[89] and that the data collector must provide the data subject, from whom data is collected, the purposes of the processing for which the data are intended.[90] The data subject also must have the right to object, on request and free of charge, to the processing of personal data relating to him/her, which the controller anticipates being processed for the purposes of direct marketing.[91]

In North America, and more specifically in the United States, the Safe Harbor[92] states that an organization must give individuals the opportunity to choose, through an opt-out procedure, whether and how personal information they provide is used, where such use is unrelated to the use(s) for which they originally disclosed it.[93] The *Telecommunications Act of 1996*[94] included a new section 222 to the *Communications Act of 1934*[95] that enacts statutory restrictions on the use of Customer Proprietary Network Information ("CPNI"), data

regarding a customer's account and usage by carriers, that restricts both 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.[96]

The *Wireless Privacy Protection Act of 2001*[97] is a bill recently introduced in the United States. It requires that a customer shall not be considered to have granted express prior authorization unless the carrier has provided in writing to the customer a clear, conspicuous, and complete disclosure of the carrier's practices with respect to the collection and use of location information, transaction information, and automatic crash identification information, before any such information is disclosed or used unless the customer has so agreed in writing.[98] Another bill introduced in the United States in July of 2001, the *Location Privacy Protection Act of 2001*,[99] requires providers of location-based services and applications to obtain a customer's express authorization before collecting, using, or retaining the customer's location information,[100] or disclosing or permitting access to the customer's location information to any person who is not a party to, or who is not necessary to the performance of, the service contract between the customer and such provider.[101] 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.[102]

In Canada, the *Personal Information Protection and Electronic Documents Act*[103] mentions that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate under the circumstances[104] and with the knowledge or consent of the individual except where inappropriate.[105] 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[106] and the form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information[107] and the ways in which an organization seeks consent, which may vary depending on the circumstances and the type of information collected.[108] The law also suggests that an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice[109] after the organization informs the individual of the implications of such withdrawal.[110]

In the telecommunications sector, the policy objectives in section 7 of the *Telecommunications Act*[111] are aiming to contribute to the protection of the privacy of persons. Since this restricts Canadian carriers, including cellular and personal communications services providers ("PCS"), from providing confidential customer information to third parties without the written consent of the customer, Bell Canada[112] and other companies applied to the Canadian Radio-television and Telecommunications Commission[113] in November 2000 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.[114]

Regulations related to spam

In the context of the Internet, spam has been an ongoing issue that has resulted in certain initiatives in Europe and the recent introduction of many anti-spam bills in the United States.

In Europe, the Electronic Commerce Directive[115] states that, with regards to unsolicited commercial communications, member states 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.[116] At the same time, it appears that the European Coalition Against Unsolicited Commercial Email[117] ("CAUCE"), a group of Internet users that have formed a coalition to promote legislation that would outlaw unsolicited commercial e-mail, is trying hard to promote the "opt-in" model as the scheme of choice.[118]

In the United States, on the Internet side, many bills have been recently introduced to regulate spam. In the last year, the bills introduced prohibit these messages from having false headers or deceptive subject lines.[119] They also require that these messages be labeled[120] and that they include opt-out instructions.[121] On the wireless side, a bill introduced in January 2001, the *Wireless Telephone Spam Protection Act of 2001*,[122] addresses the problem of unwanted wireless spam by prohibiting the use of wireless messaging systems to send unsolicited advertisements to wireless telephones.[123]

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 Web site owner responsible for sending spam.[124] Also, a recent decision from the Privacy Commissioner of Canada seems to imply that opt-in is a much better way of gathering a user's consent:[125]

> 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 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.[126]

Practical issues related to consent

Although the laws and regulations are clear on the fact that the wireless user's consent is needed prior to the using of collected location data and regarding the pushing of messages to wireless devices, they do not specify other issues including from whom the consent should be taken, and which party should be in charge of obtaining such consent. Also, the laws are not unanimous either on the method (opt-in versus opt-out procedure) or 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 advertising.

From whom do you get consent?

It may be obvious that it will be necessary to obtain consent from the wireless users prior to sending location-based advertising in order to avoid spam but should a service provider also obtain consent from a wireless user that will be tracked, even on an anonymous basis?

In order to determine the users from whom a service provider should get consent prior to tracking a wireless user, it may also be appropriate to determine "who owns this location data", issue raised by TruePosition Technology.[127] This would be one of the most highly controversial questions and one of the most critical issues facing the information economy, according to certain analysts.[128]

Who should be responsible for obtaining consent?

In the providing of location-based advertising, there would be different touch points with the consumer, the device manufacturer, the carrier and the ad serving company. Author Arasbella Hallawell raised the issue of "when the users express their choice, who should be honoring the commitment?"[129] It may make the most sense to have the same 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 on the part of the user.

How should consent be obtained?

The next issue involves the appropriate way to obtain or give such consent in order to make sure that the wireless user gave it in a meaningful manner. The Wireless Consumers Alliance Inc. is of the opinion that such consent should be provided in a clear way.[130] On 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 where a wireless user could easily click a button to opt-in or opt-out.[131] The CTIA seems to be of the opinion that there are a myriad of ways by which a service provider may satisfy the consent requirement, such as signed service agreements, Web site subscriptions, "click wrap" agreements, and user signaling via a handset or PDA.[132]

Push and Pull

Wireless data is generally accessible in two formats, pull data or push data. "Pull data" involves the process of actively requesting wireless data using a wireless device, similar to browsing for information on the wired web.[133] More specifically, this model serves the consumer by promoting free content, and involves placing advertisements on browsed wireless content so that viewers surfing the wireless web will see ads appropriate to the content they are retrieving from various Web sites.[134]

In this 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 any such transaction, such as when a wireless user calls a location-based concierge service seeking driving directions to the closest restaurant. For example, as the American Automobile Association ("AAA")[135] states, the consumers who utilize its location-based assistance service have very definite expectations that the AAA will use their location information to provide the service to which they subscribe.[136] In some cases, consent can be implied by a person's specific actions as raised in the context of the CTIA Petition, especially in emergency situations.[137] Texas 9-1-1 Agencies outlines[138] that it is of the general opinion that a caller, by dialing 911, implicitly consents to the disclosure of his/her location information.[139]

"Push data" is information sent to devices as short bursts of text, generally 160 characters or less ("SMS"), sometimes called alerts. In the case of wireless advertising, "push advertising" involves pushing advertising messages to consumers, usually in the form of an SMS.[140] Privacy and consumer rights issues surround push advertising, since it is the model that is most likely to be intrusive, as it may be unsolicited.[141] For this reason, the present paper further analyzes the privacy issues based on push location-based advertising. As a matter of fact, consent is a necessity when pushing messages to people. For example, if a retail chain broadcasts notices of sales and the geographic locations of their stores, it needs to know, with a high degree of certainty, whether the wireless user recipients are interested in receiving such information.

Opt-in vs. Opt-out

Analysts are of the opinion that the logistics of how consumers will opt-in and opt-out are not well defined and are raising several concerns.[142] It needs to be determined if the wireless user should be able to opt-in or opt-out of both the tracking and the receiving of location-based advertising.

On the Internet side, the United States seems to be promoting an opt-out approach by most e-commerce Web sites now. In Europe, and perhaps even in Canada, it seems to be more of an opt-in approach. The privacy context may be different in the wireless world, since it involves the aspect of location and the fact that a wireless device usually has one single user, making this media more intrusive than advertising on the Internet.

The Direct Marketing Association[143] ("DMA") initially promoted an opt-out approach. It recently informed the FTC that it is changing its views on this issue based on who pays for the location-based advertising. 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.[144] This type of reasoning may imply that a service provider could track a wireless user without their consent and start sending advertising messages if such user is not paying for the SMS message, which appears to be very intrusive.

When should consent be obtained?

With regards to the time of the consent, we face the same controversy already discussed. It is to be determined if the consent should take place prior to the collection of the data or prior to the use of the collected data. It has been noted that *The U.S. Telecommunications Act*[145] does not require consent prior to the collection of location data but does require that consent be given before use or disclosure of such data.[146] This would imply that a service provider may be entitled to track a wireless user and only obtain his/her consent prior to using the stored location data it has collected about such user, which seems also to be very intrusive in nature. It is interesting to note that CTIA also promotes that the consent be made manifest and express prior to the use of location data.[147]

What should be the content of consent?

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

Internet users have for years been complaining about unwanted e-mail and consumers are now concerned about spam sent to their wireless devices.[148] For this reason, the second issue of where the consent may be required from the wireless user is related to the actual receiving of the location-based advertising. For example, wireless users may opt-in to receive messages but end up being bombarded with information from all stores as they are walking into a mall.[149] London-based research and consulting firm, Ovum,[150] 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.[151] It still remains to be determined whether wireless users should provide consent regarding related issues such as how many messages they want to receive each day, from whom, and where these messages are received.

Also, once the wireless user has provided consent, it may be appropriate for him/her to know how long the consent is valid. It has been suggested that companies should focus on services where users provide explicit consent to process location data for each individual transaction.[152] This suggestion may be very impractical and a solution to avoid this may be to request that the wireless user specifies for how long the consent is valid.

Solving the Problem

It is a difficult challenge for a service provider looking to provide location-based advertising to figure out how to make an effective disclosure and obtain a meaningful consent where both are compatible with privacy protections and also comply with present laws and regulations. As a matter of fact, and as was outlined by author Arabella Hallawell 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.[153]

The existing rules are not very specific and they have different views on certain issues (such as when a disclosure should be made). Also, such rules do not take into consideration the specific nature of a service like location-based advertising and the issues surrounding it (such as the size of the screen of the wireless device). Author Robert Gellman, in his article entitled "Does Privacy Law work?", also criticizes the vagueness of the present rules. He cites the vagueness of the European Directive on privacy when it says that "personal data should be relevant to the purposes for which they are to be used and should be accurate, complete, and timely".[154]

The following sections are meant to propose a way for service providers, looking to collect location data from wireless users in order to provide these users with personalized location-based advertising, to also provide wireless users with an effective disclosure and obtain valid consent from them.

Effective and full disclosure

Even if the carrier uses the wireless users' location data in order to provide these users with telecommunications services, it would still make sense for the service provider using the same location data to inform the wireless user on the issues surrounding the tracking, collection and storage of this data in the event that these

activities are not part of regular telecommunications services.

Receiver of disclosure

As previously discussed, there are two types of consent required: the first one relating to the tracking and the collection of location data from the wireless users with all of its implications such as storage- and security-related issues, and the second type relating to the consent of the wireless user to receive location-based advertising.

With regards to the first type of consent related to tracking, there are two types of wireless users that could be tracked. The first includes wireless users who are being tracked on a personal basis, meaning that their identities are known. This type clearly needs to obtain the effective disclosure with regards to the tracking. On the other hand, it is not as clear of the second, which is the type of wireless users who would be tracked anonymously.

On this last issue, obtaining disclosure may depend upon which party owns the location data. With regards to such ownership, we appear to be in the presence of a co-ownership of the location 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 provide that the consent of the user be obtained prior the collection or use of such data.

This interpretation seems to be in line with the *Location Privacy Protection Act of 2001* that 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.[155] At the same time, we may not have to take a clear position regarding this ownership since in the event that carriers use or collect this location data for other purposes than providing standard telecommunications services to wireless users, the consent of the user is required.

As previously mentioned, since in the case of location-based advertising the location data used may either contain or merge with PII, it may be useful to also provide disclosure to the wireless user prior to tracking, whether anonymous or not.

As for the second type of consent related to the receiving of location-based advertising, wireless users clearly need disclosure of the service provider relating to the collection of their location data, since they will provide their consent based on the service provider's policies relating to the storage, security and transfer of their data.

Party responsible for providing disclosure

The party in charge of providing disclosure to the wireless users that they are being tracked, and where such location data is collected and stored, should be the carriers. This is for many reasons, including the fact that the carriers provide the network service and thus already own the relationship with their subscribers.[156] CTIA seem 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.[157]

The Electronic Privacy Information Center ("EPIC"),[158] a Washington-based privacy group, has offered the contrary opinion that wireless users should be able to get location-based advertising and services from anyone and not necessarily from their carrier.[159] Even if such a statement were relevant, implementing this could only cause confusion. The location-based advertising service provider, by partnering with the carrier, most probably would benefit from the trusted relationship that the wireless user already has with his/her carrier. Otherwise, the wireless user dealing with different parties all providing different notices for each new application would invite chaos. Since the carrier already has the control of such a relationship, it may be viewed as the distribution channel for any new wireless service to be offered to wireless users.

Also, a carrier clearly has a trusted relationship with its subscribers, whether it is 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.[160] This places carriers in the position of a "trusted agent" with respect to its subscribers.

Finally, carriers generally treat customer information as a valuable asset and trade secret. They share the customer's interest in safeguarding and protecting the information, which as a principle is without controversy.[161] Several carriers such as Sprint PCS[162] and AT&T Corporation[163] say they use the existing data on the location of a phone, which is now based on the nearest cellular tower, only to make connections and bill calls. As a matter of fact, Sprint PCS has emitted the opinion that carriers have every incentive to listen carefully to what their customers want[164] and agrees with Verizon Wireless[165] that carriers have a powerful incentive to adhere to a privacy-oriented, consumer-friendly approach when it comes to the use of personal or location data. The wireless marketplace is extraordinarily

competitive and carriers that fail to maintain the trust of their subscribers will suffer severe consequences.[166]

Way of providing the disclosure

For reasons related to the size and limitations of the wireless phone screen and reasons discussed above, the disclosure should not be done on the wireless device. Also, and as was proposed by CDT, 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.[167]

CTIA pointed out in its Petition that there are several ways in which a service provider could inform a wireless user about its location information practices. 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 Web site, or in a letter sent to subscribers:[168]

> 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.[169]

Others, like AT&T Labs Research, believe that the disclosure should be made by service contracts.[170] 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 in the carrier's store or even on the carrier's Web site and should be made in writing.[171] Such disclosure should not necessarily have to be made on paper in the case of Web site consent, which would still make it a valid consent,[172] according to companies like NetCoalition.[173]

Time of the disclosure

The disclosure should be made prior to the collection of location data and not prior to use in order for such disclosure to comply with all European and North American laws and regulations[174] and to avoid any potential privacy breaches.

Content of the disclosure

Prior to the tracking of the wireless user and the collection of his/her location data, and whether the wireless user will be tracked anonymously or not, the disclosure from the carrier should cover the following features in order to be considered appropriate, and in order to comply with North American and European laws and regulations:

- **The collection of the data:** The carrier should inform the wireless user of the fact that it is collecting data related to him/her,[175] given that such collection may not be part of providing standard telecommunications services.
- **Type of data:**[176] The carrier should inform the wireless user about the type of data being collected when the user is using his/her 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. 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:**[177] 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. The type of tracking technology used with relevant information should be detailed and disclosed.
- **Collector's identity and place of business:**[178] 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:**[179] As previously mentioned, the 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[180] and that it is also accurate, complete, and up to date.
- **Use or purpose of the data:**[181] The carrier should specify the purpose of the location data and explain how such data will be used.[182] Furthermore, the carrier should undertake to inform the wireless user that s/he would be informed of any change in the use or purpose of the collection of the data,[183] before such change becomes effective.
- **Storage of the data:**[184] The carrier should inform the wireless users of its policies regarding the storage of data[185] and the retention or processing of the data,[186] including whether any PII is stored permanently.[187] Even if the wireless user renews the authorization, he/she should be told how long the location data is retained before being purged.[188]
- **Security of the data:**[189] 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[190] and, as the case may be, the details regarding the security measure adopted for the storage, such as the type and strength of encryption.

- **Access to the personal data:**[191] The means for wireless users of gaining access to personal information held by the service provider[192] and the system to update and correct any inaccuracy of the data collected should be disclosed to the wireless user. Also, the carrier should inform the wireless user that it may access his/her Static Profile data in order to make any changes and updates through a specific and simple mechanism.
- **Transfer to third party:**[193] 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,[194] collectors of information, profiling and "ad serving organizations".[195] Wireless users should also be informed of these third parties' policies with regards to the disclosure of the collected data.[196]
- **Procedure to complain:**[197] The wireless users should be informed of the system or procedure that they might use to complain about the location-based advertising service, the carrier, the service provider, 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.
- **Update or change in the Privacy Policy:**[198] The carrier should specify that it will not change its privacy policy prior to sending either a letter or an e-mail entitled "Update to the Privacy Policy" to the wireless user. 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**[199] **/ Implications of an Opt-out:**[200] The carrier should inform the user that it may withdraw his/her 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/she does opt out, he/she is effectively opting out in several respects: (i) the user will no longer receive location-based messages; and (ii) he/she will no longer be profiled. Furthermore, all additional information provided by the user at opt-in (Static Profile data) and location data will be deleted from the service provider databases.
- **Request of deletion:** The wireless user should be informed of the procedure available to him/her regarding the potential request to delete his/her Static Profile information as well as his/her stored historical location data and what the carrier and the service provider intend to do with such requests.[201]

Once all of these above-mentioned issues are covered, the carrier shall provide the wireless user with the option to refuse that s/he be tracked for location-based service purposes.

- **Choice and consent:**[202] The choices available to a wireless user regarding the collection[203] 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[204] and to receiving unsolicited communications for such purposes.[205]
- **Period of validity for consent:** The wireless user should be informed by the carrier as to how long his/her 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 advertising after having received a disclosure from the carrier that covers the above-mentioned issues, the carrier shall inform such user whether his/her **responses** to the messages or **to wireless advertising** will be recorded and tracked. 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[206] survey panel of mobile phone and wireless Internet users confirmed their interest and opinion towards wireless advertising. It is interesting to note that nearly all of these panelists wanted to ensure the privacy of any data collected on their responses to wireless advertising.[207]

Meaningful Choice and Consent

Once wireless users obtained an effective disclosure, they should have the opportunity to choose whether they wish to be tracked for location-based advertising purposes, whether they actually wish to receive location-based advertising, and to what extent. A wireless user

pushed with a discount offer on his/her wireless device while walking past a specific store may very well appreciate the benefits of tracking. However, 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 advertising messages on their wireless device unless such messages are anticipated.

Provider of consent

This type of consent would come from two classes of people: the first class includes wireless users that will be tracked, whether or not is it done anonymously, and the second class includes wireless users that will receive advertising services on their wireless device.

Regarding the first class of people, for reasons already expressed in this article — and since, in the case of advertising, the location data used may either contain PII or a threat that location data will be merged with PII — it may be useful and appropriate to obtain the consent of the wireless user prior to the collection of his/her location data, whether the tracking is done anonymously or not.

The second class of people who need to provide their consent on all the issues (that will be further discussed in this article) and prior to receiving location-based advertising includes the wireless users who will receive advertising services and content on their wireless device.

Party responsible for obtaining consent

The carrier should be the party not only providing the disclosure to the wireless users regarding the tracking, but also obtaining their consent related to this tracking and to the receiving of location-based advertising. TRUSTe[208] agrees with the fact that the carrier may ultimately be in the best position to be a clearinghouse for anyone who wants to advertise on their network.[209]

Way of obtaining consent

Carriers in the United States have expressed the opinion that the FCC[210] should not prescribe a uniform way to provide notice and consent. As a matter of fact, Verizon Wireless,[211] believes that notice and consent can be communicated effectively in any number of ways and that carriers must have the flexibility to tailor notice and consent practices.[212] Sprint PCS[213] shares the same opinion and states that choosing one consent procedure over another is not a decision this Commission or any other regulatory needs to — or should — make, at least at this point in time.[214] The best procedure may be that the consent be made with the carrier at its point of sale or on its Web site following an effective disclosure. 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 participate in the location-based advertising service.

Push and Pull

With regards to the pull model, there is an implicit consent to the disclosing of the location. This type of consent, though 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 service provider is storing location data, based on the wireless user pull requests, disclosure should be made prior to the collection of such data and consent would be required by the wireless user. With regards to the push model, the section below will further describe the details regarding the consent required prior to the collection or use of location data and the receiving of location-based advertising.

Opt-in vs. Opt-out

Wireless users should be getting the opportunity to opt-out of such tracking and should opt-in to receiving location-based advertising and messages.

Tracking and collection of location data

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, which would be in line with the privacy standards advocated by wireless trade groups such as the CTIA.

In the event that the wireless users are being tracked anonymously, the wireless users should, once they have obtained an effective disclosure, be able to opt-out of such tracking. As a matter of fact, there should be a black list for certain wireless users who may not want to be tracked by their carrier or a service provider — for example, if they have been a victim of stalking and/or if they feel uncomfortable with the idea of their historical movements being tracked and stored — even if all of this is done on an anonymous basis. It is interesting to note that the industry's position is that an opt-out procedure may also adequately protects 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.[215] Carriers like Sprint PCS seem to be of the opinion that opt-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. Ensuing market experience may reveal that consumers find opt-in procedures unreasonably interfere with their ability to timely obtain and use certain desired services.[216]

Receiving location-based advertising

In wireless advertising, the concept of acceptance is very important to confirm that wireless messages are welcome.[217] Cahners In-Stat Group recently surveyed its panel of wireless phone and wireless Internet users to determine their interest and opinion towards wireless advertising.[218] Panelists noted the importance of having the ability to opt-in for wireless advertising with 58 per cent of wireless phone users and 77 per cent of wireless Internet users finding it important to have this option.[219] Confirmed opt-in, also known as double opt-in, is the process of verifying a user's permission in order to ensure that wireless push advertising is not accidentally or maliciously sent to the user's wireless device.[220] For example, after receiving permission from a wireless user, the service provider may send a message to the wireless user to which s/he must positively reply in order to confirm permission to start receiving push messaging.[221] Industry privacy associations like the Wireless Location Industry Association ("WLIA"),[222] the Wireless Advertising Association[223] working under the name of Mobile Marketing Association ("MMA") since January of 2002,[224] 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 practical and seem to be promoting a confirmed opt-in approach for the wireless space[225] in general. Equipment manufacturers like Nokia[226] seem to agree with such a position.[227]

In the event that consent is appropriately obtained, and after obtaining effective disclosure, there may not be any 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 would probably be more relevant and should take place in a Web site environment when the identity of the user is unknown and anyone could opt-in on behalf of another person using his/her e-mail address or in the event that the consent is obtained through a wireless device, which procedure is not the best one for reasons already discussed.

For these reasons, the wireless user should simply opt-in to receive location-based advertising, which is a process that requires active choice on the part of the wireless user to express permission. Such mechanism is adequate to avoid spam and would comply with European and North American laws and regulations already discussed.[228]

Time of consent

The wireless user's consent should be obtained before the collection of location data, unless it is being tracked anonymously. In this last case, the wireless user should be entitled to opt-out of such tracking as soon as it is informed of the tracking.

The wireless user shall also provide his/her consent prior to the use of location data, meaning prior to receiving advertising that is location-based. Such user will need to have opted-in to that specific advertising service.

Content of consent

At the same time, and following Ovum's[229] suggestion, service providers offering location-based advertising should give the wireless user a strong element of control over the type, frequency and timing of advertisement delivery.[230] The wireless user's consent should be provided on the following issues:

- **Number and frequency of messages**: Wireless users should be able to specify how many messages they wish to receive a day, choosing a minimum, a maximum, and a range. For example, a wireless user might agree to receiving more messages on the weekend and less during the week.
- **Provider of messages**: Wireless users should be able to specify that they will accept receiving messages but only from certain types of content providers, even to the point of specifying names of advertisers allowed to push content through their wireless device. At the same time, users should be in a position to specify the type of advertisers from whom they do not wish to receive messages. Cahners In-Stat Group[231] recently surveyed its panel of mobile phone and wireless Internet users to determine their interest and opinion towards mobile advertising:[232]

> … 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.[233]

- **Type of messages**: Wireless users should be able to specify the type of message they wish to receive — for example, content and advertising related to sports — as well as the type of content they do not wish to receive.
- **Time of messages**: Wireless users should be able to specify that they wish to receive advertising messages only at certain times; for example, only during the day, only over the weekends, only during the evenings.
- **Location of messages**: Wireless users should be able to specify that they wish to receive advertising messages based on when they are at certain locations; for example, only when they are downtown or at the office but never when they are at home.

The DMA[234] 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 be at all reluctant 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**, which practice may be relevant for any push message sent on a wireless device. Secondly, and as already discussed, the messages sent should be subject-relevant. Through the use of profiling, the service provider should send the right message to the right person at the right time, thereby increasing the efficiency of the medium and eliminating wireless spam. Finally, the wireless users should be informed **on how they may file a complaint** about the location-based advertising service. Users should also be able to specify the **length of time** their consent is valid, be able to request at any time that they do not wish to be part of the location-based advertising service (**opt-out**), and also be entitled to request that their **location data be deleted** in such a case.

Conclusion

Location-based advertising presents a unique opportunity for advertisers to bridge the prediction of wireless users' preferences and buying patterns with direct marketing targeted to the exact moment and location of the consumer. This relationship between the marketer and the consumer can be mutually beneficial, but its desirability and acceptability depends on the consumer's control over the advertising to which they are exposed. As a matter of fact, 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 these users against their will or send them unsolicited messages based on their geographical position.

An independent analysis of the competitive forces, revenue models and wireless advertising possibilities, revealed the fact that the wireless device is a personal tool that contains telephone numbers and dates, and that wireless users expect to operate it without any disturbance to their privacy, so that the level of intimacy becomes the basis for permissive marketing.[235]

Consumers are already dissatisfied with the volume of unsolicited marketing directed to them by mail, telephone and e-mail.[236] Consumer dissatisfaction is likely to be heightened when the advertisements 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, these consumers will feel as though there is an omnipresent surveillance of their activities by companies they do not know.

In order for wireless users to provide meaningful consent prior to receiving location-based advertising, they need to obtain an appropriate and effective disclosure regarding all issues surrounding the tracking, the collection, and the use of their personal or location data through wireless technologies. Even though the present laws and regulations provide a general legal framework, the details of translating these privacy laws into actual business and information technology practices will be the greatest challenge for enterprises that will have to take a step in making sure that they have obtained meaningful consent from the wireless users before providing them with these new types of services.

Finally, it is one thing to actually disclose the tracking to the wireless users but it will be interesting to see how the industry, and perhaps even the government, may play a role in educating wireless users on these complex issues of opt-in, opt-out, security and privacy in a form that is easy to understand and to obtain so that they can make an intelligent and informed choice.

Notes:

[1] Mike McGuire, *Moble Business Markets: What Can't Users Live Without*, GARTNER INC. Symposium ITxpo 2001, Orlando, Florida: October 2001, at 2.

[2] NTT DoCoMo is a provider of wireless voice and data communications in Japan. <http://www.nttdocomo.com/>

[3] Goldman Sachs is a global investment banking and securities firm. <http://www.gs.com/>

[4] Goldman Sachs, *Technology: Mobile Internet* MOBILE INTERNET PRIMER, United States: July 14, 2000, at 5.

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

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

[7] Gary W. Ozanich, *The Wireless Marketing Opportunity*, KELSEY GROUP (The): April 10, 2001, at 1.

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

[9] <http://www.verizonwireless.com/>

[10] <http://www.wwireless.com/>

[11] <http://www.sprintpcs.com/>

[12] <http://www.alltel.com/>

[13] <http://www.nextel.com/>

[14] 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>

[15] 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/>

[16] 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/>

[17] Double-Click is a provider of broad range of technology, media, direct marketing, e-mail and research solutions. <http://www.doubleclick.com>

[18] Engage is a content management solutions provider. <http://www.engage.com/>

[19] Quios is a global SMS distributor. <http://www.quios.com/>

[20] *Supra* note 17.

[21] Quios and Engage, *The Efficacy of Wireless Advertising* Industry Overview and Case Study, 2000, at 2.

[22] The Center for Democracy and Technology is an organization that works to promote democratic values and constitutional liberties in the digital age. <http://www.cdt.org/>

[23] 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, at 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.)

[24] Kevin Mabley, *Privacy vs. Personalization — Personalization: A threat to privacy?* CYBER DIALOGUE INC., 2000, at 1.

[25] <http://www.privacytimes.com/>

[26] Steve Stutman, President and CEO, ClickaDeal.com, 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, at 34.

[27] 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>

[28] *Supra* note 5.

[29] Carsten Schmidt, *Shortcuts to Mobile Location Services*, THE FORRESTER REPORT, May 2001, at 3.

[30] *Supra* note 25, Lorrie Faith Cranor, AT&T Labs research, at 5.

[31] Windwire has developed a technology that allows advertisers to deliver targeted offers for each consumer's wireless device. <http://www.windwire.com/>

[32] *Supra* note 7, at 24.

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

[34] *Id.* at 3.

[35] *Supra* note 28.

[36] Mobile Marketing Association, *MMA Guidelines on Privacy and Spam*, Phase 1, November 7, 2000. <http://www.waaglobal.org/>

[37] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980.

[38] *Id.* Article 9.

[39] *Id.* Article 12.

[40] European Union, 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 (October 24, 1995).

[41] *Id.* Article 6 a).

[42] 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), Brussels, 12-7- 2000, COM (2000) 385 Final, 2000/0189 (COD). <http://europa.eu.int/eur-lex/en/com/dat/2000/en_500PC0385.html>

[43] 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>

[44] *Supra* note 41, Article 9.

[45] *Id.* Article 13.

[46] U.S. Department of Commerce, *Safe Harbor Agreement*, November 1, 2000. <http://www.export.gov/safeharbor/>

[47] *Id.* Article 1.

[48] *Id.*

[49] The *Wireless Privacy Protection Act of 2001*, HR 260, Introduced on January 30, 2001 by Mr. Frelinghuysen which was referred to the Committee on Energy and Commerce.

[50] *Id.* Article 3.

[51] *Id.* Article (1) (A).

[52] *Id.* Article (1) (B).

[53] *Location Privacy Protection Act of 2001*, S 1164, Introduced on July 11, 2001 by Sen. John Edwards, Congressional Record.

[54] *Id.* Section 3, Article (b)(1)(A).

[55] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

[56] *Privacy Code a must for global economy*, Focus (Canadian Standard Association), Spring 1992.

[57] *Supra* note 54, Schedule 1, Section 5, Article 4.2.3.

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id.* Schedule 1, Section 5, Article 4.8.

[63] *Id.* Article 4.8.2 (a).

[64] *Id.* Article 4.8.2 (b).

[65] *Id.* Article 4.8.2 (c).

[66] *Id.* Article 4.8.2 (d).

[67] *Id.* Article 4.8.2 (e).

[68] *Id.* Article 4.8.3.

[69] *Supra* note 12.

[70] 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, at 2.

[71] *Supra* note 21.

[72] <http://www.fiderus.com/>

[73] *Supra* note 25, Alan Davidson, attorney, Center for Democracy and Technology, at 9; and *supra* note 25, Donald Bromley, Fiderus Strategic Security and Privacy Services, at 10.

[74] Wireless Consumers Alliance, Inc. is an independent, non-profit organization that was formed to promote and serve the interests of consumers of wireless services in the United States. <http://www.wireless-consumers.org/>

[75] *Supra* note 69, Wireless Consumers Alliance, Inc., Comment, April 6, 2001, 8 pages, at 2.

[76] *Supra* note 36, Article 9; *supra* note 45, Article 1; and *supra* note 54, Schedule 1, Section 5, Article 4.2.3.

[77] *Supra* note 48, Article (1)(B).

[78] <http://www.wow-com.com/>

[79] 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, at 9.

[80] *Supra* note 69, Cellular Telecommunications Industry Association, *Petition*, November 22, 2000, 12 pages, at 9.

[81] AT&T Wireless, *AT&T Wireless Privacy Policy*, Effective February 7, 2002. <http://www.attws.com/privacy/>

[82] Section entitled "Updating this Policy" of the AT&T Wireless, AT&T Wireless Privacy Policy, Effective February 7, 2002. <http://www.attws.com/privacy/>

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

[84] *Supra* note 25, Dana Rosenfeld, Office of Director at the Bureau of Consumer Protection, p. 9.

[85] *Supra* note 36.

[86] *Id.* Article 7.

[87] *Id.* Article 10 a).

[88] *Supra* note 39.

[89] *Id.* Article 7 a).

[90] *Id.* Article 10 b).

[91] *Id.* Article 14 b), and Articles 11 1) and 12 1).

[92] *Supra* note 45.

[93] *Id.* Article 2.

[94] The *Telecommunications Act of 1996*, 47 U.S.C. Section 222 Privacy of customer information.

[95] The *Communications Act of 1934*, 47 U.S.C.

[96] Section 222 was again amended by the *Wireless Communications and Public Safety Act of 1999*, House of Representatives, H.R. 438 & H.R. 514, 106th Cong. First Session, February 3, 1999.

[97] *Supra* note 48.

[98] *Id.* Article (2).

[99] *Supra* note 52.

[100] *Id.* Section 3, Article (b)(1)(B)(i).

[101] *Id.* Article (b)(1)(B)(ii).

[102] *Id.* Article (b)(4)(A).

[103] *Supra* note 54.

[104] *Id.* Article 5(3).

[105] *Id.* Schedule 1, Section 5, Article 4.3.

[106] *Id.* Article 4.3.2.

[107] *Id.* Article 4.3.4.

[108] *Id.* Article 4.3.6.

[109] *Id.* Article 4.3.8.

[110] *Id.*

[111] Section 7, *Telecommunications Act, 1993.* c. 38. <http://lois.justice.gc.ca/en/T-3.4/text.html>

[112] 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/>

[113] The CRTC is an independent agency responsible for regulating Canada's broadcasting and telecommunications systems. <http://www.crtc.gc.ca/>

[114] 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>

[115] European Commission, *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.

[116] *Id.* Article 7 (2).

[117] EuroCAUCE <http://www.euro.cauce.org/en/index.html>

[118] <http://www.euro.cauce.org/en/countries/index.html>, and <http://www.euro.cauce.org/en/optinvsoptout.html>

[119] *The Anti-Spamming Act of 2001*, H.R. 718, 107th Cong., 1st Session, June 5, 2001; Section 5, (a) (2), *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act of 2001*, S. 630, 107th Congress, 21st Session, March 27, 2001; and Section 4, *The Unsolicited Commercial Electronic Mail Act of 2001*, H.R. 95, 107th Congress, 1st Session, January 3, 2001.

[120] Section 5, (a) (5), *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act of 2001*, S. 630, 107th Congress, 21st Session, March 27, 2001; Section 2 (a) (1), *The Netizens Protection Act of 2001*, H.R. 3146, 107th Congress, 1st Session, October 16, 2001; and Section 5 (a) (3), *The Unsolicited Commercial Electronic Mail Act of 2001*, H.R. 95, 107th Congress, 1st Session, January 3, 2001.

[121] *Id.*

[122] The *Wireless Telephone Spam Protection Act of 2001*, H.R. 113, 107th Congress, 1st Session, January 3, 2001.

[123] *Id.* Section 2(5) and Section 3(a)(1)(e).

[124] *1267632 Ontario Inc. c. Nexx Online Inc.*, Ontario Superior Court, July 9, 1999.

[125] 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>

[126] *Id.*

[127] TruePosition technology locates the new wireless world, enabling carriers, application providers, and enterprises to deliver value-added location-based services to their customers. <http://www.trueposition.com/>; *supra* note 25, Michael Amarosa, VP Public Affairs, True Position Inc., at 28.

[128] Arasbella Hallawell, *Mr. President, It's time for New Privacy Protection methods*, GARTNER INC., Research Note, March 1, 2001, at 1.

[129] *Supra* note 25, Lawrence Ponemon, Pricewaterhouse, at 6.

[130] *Supra* note 69, Wireless Consumers Alliance, Inc., *Comment*, April 6, 2001, 8 pages, at 2.

[131] 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>

[132] *Supra* note 69, Cellular Telecommunications Industry Association, *Petition*, November 22, 2000, 12 pages, at 9-10.

[133] *Supra* note 7, p. 2.

[134] *Id.* at 4.

[135] The American Automobile Association is one of the largest motoring services organization and leading provider of roadside assistance throughout the U.S. and Canada.

[136] *Supra* note 69, American Automobile Association, *Reply to Comments*, April 24, 2001, 9 pages, at 4.

[137] *Id.* EPIC, Reply to Comments, April 24, 2001, 18 pages, at 8.

[138] *Id.* The Texas 9-1-1 Agencies, *Comment*, April 6, 2001, 5 pages, at 3.

[139] *Supra* note 131, at 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, (Sept. 10, 1996) (filed for CC Docket No. 94-102).

[140] *Supra* note 7, at 4.

[141] Rosalie Nelson, *Mobile Advertising: building alternative revenue streams*, OVUM REPORT, Short Report, June 20, 2000, at 7.

[142] *Supra* note 131.

[143] The Direct Marketing Association (The DMA) is the oldest (1917) trade association for users and suppliers in the direct, database and interactive marketing field. <http://www.the-dma.org/>

[144] *Supra* note 25, Jerry Cerasale, Senior VP for Government Affairs at the Direct Marketing Association, at 38.

[145] *Supra* note 94.

[146] *Id.* Section 222 (c)(i).

[147] *Supra* note 131, at 10.

[148] 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>

[149] 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>

[150] <http://www.ovum.com/>

[151] Rosalie Nelson, Neil Ward-Dutton and BG, *Wireless Marketing: Rhetoric, reality & revenues*, OVUM REPORT, June 2001.

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

[153] *Supra* note 4.

[154] ROBERT GELLMAN, *Does Privacy Law work?, Technology and Privacy: The New Landscape*, edited by Philip E. Agre and Marc Rotenberg, 1998, p. 193, at 197.

[155] *Location Privacy bill Introduced*, ALLNETDEVICES, 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> As a matter of fact, the 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". This term is further defined as a collection of location data relating to a group or category of customers from which individual customer identities have been removed, which seems to imply that a service provider may collect and use the location data of anonymous wireless users without informing such users that it is tracking them (see *supra* note 52, Section 3, Articles (b)(2)(D) and (f)(1)).

[156] *Supra* note 25, Donald Bromley, Fiderus Strategic Security and Privacy Services, at 11.

[157] *Supra* note 69, Cellular Telecommunications Industry Association, *Comment*, April 24, 2001, 21 pages, at 6.

[158] <http://www.epic.org/>

[159] *Supra* note 69, EPIC, Reply to Comments, April 24, 2001, 18 pages, at 9-10.

[160] *Supra* note 94, and Section 7, *Telecommunications Act, 1993*, c. 38, Canada. <http://lois.justice.gc.ca/en/T-3.4/text.html>

[161] *Supra* note 69, Cellular Telecommunications Industry Association, *Comment*, April 24, 2001, 21 pages, at 14.

[162] *Supra* note 10.

[163] <http://www.att.com/>

[164] *Supra* note 69, Sprint PCS, Comment, April 6, 2001, 25 pages, at 10.

[165] *Supra* note 8.

[166] *Supra* note 69, Sprint PCS, *Reply to Comments*, April 24, 2001, 16 pages, at 10, referring to page 8 of the Verizon Wireless comments.

[167] *Supra* note 22, at 10.

[168] *Supra* note 131, at 9-10.

[169] *Id.*

[170] *Supra* note 25, Lorrie Faith Cranor, AT&T Labs Research, at 7.

[171] *Supra* note 48, Articles (1)(A) and (2).

[172] *Supra* note 69, Net Coalition, Reply Comments, April 24, 2001, 11 pages, at 7-8.

[173] NetCoalition.com is an organization committed to building user confidence in the Internet through responsible market-driven policies. <http://www.netcoalition.com/>

[174] *Supra* note 36, Article 9; *supra* note 45, Article 1; and *supra* note 54, Articles 5(3) and 7.

[175] *Supra* note 36, Article 7; *supra* note 45; Article 2; *supra* note 48; Article (2); *supra* note 52, Section 3, Article (b)(1)(B)(i); and *supra* note 54, Articles 5(3) and 7.

[176] Article 6(4) and 9(1), Council of the European Union, Common Position adopted by the Council on January 28, 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); *supra* note 45, Article 1; *supra* note 48, Article (1)(A); and *supra* note 54, Schedule 1, Section 5, Article 4.8.2(c).)

[177] *Supra* note 45, Article 1.

[178] *Supra* note 36, Article 12; Article 13, Council of the European Union, Common Position adopted by the Council on January 28, 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); *supra* note 54, Schedule 1, Section 5, Article 4.8.2(a).

[179] *Supra* note 35.

[180] *Supra* note 69, Wireless Advertising Association, Comment, April 6, 2001, 8 pages, p. 4.

[181] *Supra* note 36, Article 12; *supra* note 39; Article 6(a); Article 6(3) and 9(1), Council of the European Union, Common Position adopted by the Council on January 28, 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); *supra* note 45, Article 1; *supra* note 48, Article (1)(A); *supra* note 52, Section 3, Article (b)(1)(A); and *supra* note 35.

[182] In the case of location-based advertising, the carrier should specify that such data will be used in order to profile wireless users based on their historical and behavioral location patterns and provide them with relevant location-based advertising that the users have agreed to receive.

[183] *Supra* note 39, Article 26(a); *supra* note 45, Article 3; and *supra* note 54, Schedule 1, Section 5, Article 4.2.4.

[184] *Supra* note 35; Wireless Location Industry Association, Draft WLIA Privacy Policy Standard (November 2001). <http://www.wliaonline.org/indstandard/privacy.html>

[185] *Supra* note 22, at 8.

[186] Articles 6(4) and 9(1), Council of the European Union, Common Position adopted by the Council on January 28, 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); *supra* note 52, Section 3, Article (b)(1)(A); and Wireless Location Industry Association, Draft WLIA Privacy Policy Standard (November 2001). <http://www.wliaonline.org/indstandard/privacy.html>

[187] *Supra* note 179, p. 4.

[188] *Supra* note 69, Sirf technology Inc., Notice, April 30, 2001, 14 pages, p. 9-10.

[189] *Supra* note 35, Wireless Location Industry Association, Draft WLIA Privacy Policy Standard (November 2001). <http://www.wliaonline.org/indstandard/privacy.html>

[190] *Supra* note 179, p. 4.

[191] *Supra* note 52, Section 3, Article (b)(1)(A); *supra* note 54, Schedule 1, Section 5, Article 4.8.2(b); *supra* note 188.

[192] *Supra* note 54, Schedule 1, Section 5, Article 4.8.2(b).

[193] Articles 6(4) and 9(1), Council of the European Union, Common Position adopted by the Council on January 28, 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); *supra* note 45, Article 1; *supra* note 52, Section 3, Article (b)(1)(A); *supra* note 54, Schedule 1, Section 5, Article 4.8.2(3); *supra* note 35; and *supra* note 188.

[194] *Supra* note 179, p. 4.

[195] *Id.*

[196] *Supra* note 52, Section 3, Article (b)(1)(A).

[197] *Id.* and *supra* note 54, Schedule 1, Section 5, Article 4.8.2(a); and Article 13, Council of the European Union, Common Position adopted by the Council on January 28, 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).

[198] *Supra* note 188.

[199] Articles 6(3) and 9(1), Council of the European Union, Common Position adopted by the Council on January 28, 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 *supra* note 54, Schedule 1, Section 5, Article 4.3.8.

[200] *Supra* note 54, Schedule 1, Section 5, Article 4.3.8.

[201] More specifically, the carrier and the service provider should confirm to the wireless users that they will be able at any time to request that such data be deleted through the a specific mechanism.

[202] *Supra* note 45, Article 1; and *supra* note 188.

[203] *Supra* note 179, p. 4.

[204] *Supra* note 39, Article 14(b); 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 January 28, 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).

[205] Article 13, Council of the European Union, Common Position adopted by the Council on January 28, 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).

[206] 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/>

[207] 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>

[208] TRUSTe is an independent, non-profit privacy organization which mission is to build users' trust and confidence on the Internet. <http://www.truste.org/>

[209] *Supra* note 25, Robert E. Lewin, President and CEO, TRUSTe, at 79.

[210] The FCC is an independent United States government agency, directly responsible to Congress and established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. <http://www.fcc.gov/>

[211] *Supra* note 8.

[212] *Supra* note 69, Verizon Wireless, Comment, April 6, 2001, 12 pages, at 5.

[213] *Supra* note 10.

[214] *Supra* note 163, at 9.

[215] 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>

[216] *Supra* note 163, at 9.

[217] *Supra* note 20; and *supra* note 150, at 1.

[218] *Supra* note 205.

[219] *Id.*

[220] *Supra* note 35.

[221] *Supra* note 179, at 2.

[222] The Wireless Location Industry Association (WLIA) regroups companies providing hardware, software, services and other products related to the new ability to locate the precise origin of wireless radio signals and provides services to members around the world as this new industry emerges and offers business references and information to the public and to decision-makers. <http://www.wliaonline.org/indstandard/privacy.html>

[223] The Mobile Marketing Association (MMA) is a global industry trade association devoted to hand held device manufacturers, carriers & operators, software providers, agencies, retailers and advertisers and service providers of mobile wireless marketing and advertising. Originally formed in May 2000 with a merger of the WAIA (Wireless Advertising Industry Association) and the IAB's (USA) Wireless Task Force, the MMA is now operating independently to address the challenges facing the wireless industry. <http://www.mmaglobal.com>

[224] MMA press release, *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*, January 10, 2002. <http://www.waaglobal.org/press/merger1-10_press.html>

[225] Wireless Location Industry Association, Draft WLIA Privacy Policy Standard, November 2001, <http://www.wliaonline.org/indstandard/privacy.html>, *supra* note 35, and *supra* note 69, Location Privacy Association, Reply Comments, April 24, 2001, 12 pages, at 5.

[226] Nokia is a mobile phone supplier and a supplier of mobile and fixed telecom networks including related customer services. <http://www.nokia.com/>.

[227] *Supra* note 69, Nokia Inc., Comment, April 6, 2001, 6 pages.

[228] *Supra* note 39, Articles 7(a) and 10(b), *supra* note 36, Articles 7 and 10(a), and *supra* note 45, Article 2.

[229] *Supra* note 149.

[230] *Supra* note 150.

[231] *Supra* note 205.

[232] *Supra* note 206.

[233] *Id.*

[234] *Supra* note 142.

[235] INSEAD, *The New Wireless Economy, An independent Analysis of the Competitive Forces, Revenue Models and Wireless Advertising Possibilities*, 2001, at 48.

[236] 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>