Location Technologies: Mobility, Surveillance and Privacy

A Report to the
Office of the Privacy Commissioner of Canada
under the Contributions Program

March 2005

The Surveillance Project

c/o Department of Sociology
Queen's University
Kingston, ON K7L 3N6
(613) 533-6000, ext. 78867
(613) 533-6499 FAX
surveill@post.queensu.ca
http://www.queensu.ca/sociology/Surveillance

Authors and Acknowledgements

Authors:

David Lyon
Department of Sociology
Queen's University

Stephen Marmura
Post-doctoral fellow
The Surveillance Project
Queen's University

Pasha Peroff
Project Researcher
The Surveillance Project
Queen's University

The Surveillance Project gratefully acknowledges the work of the following individuals in the preparation of this report: Martin French, David Lavin, Jason Pridmore, Joan Sharpe, Shane Simpson and Emily Smith.

The Surveillance Project researches the ways in which personal data are processed. We explore why information about people has become so important in the 21st century and what are the social, political and economic consequences of this trend. Questions of 'privacy' and of 'social sorting' are central to our concerns. For more information, please visit: **http://www.queensu.ca/sociology/Surveillance**

Note: **Coloured text** indicates term is found in the Glossary.

Contents

Executive Summary

Location technologies have been developed to facilitate and regulate rising rates of mobility in the countries of the global north, including Canada, yet it seems clear that their advent also poses fresh challenges for privacy, security, civil liberties and social justice.

This report on location technologies and their social impact is inspired by the recent advent of real-time tracking technologies that create new concerns for Canadians and for Canadian policy provisions. As location technologies are becoming increasingly important in the early twenty-first century, citizens and policy makers need to prepare for the likely outcomes of this new technology.

Our findings are timely because they outline the potential significance and consequences of location technologies just as political, economic, social and cultural pressures are beginning to stimulate the growth of markets in tracking devices. Location technologies have been developed to facilitate and regulate rising rates of mobility in the countries of the global north, including Canada, yet it seems clear that their advent also poses fresh challenges for privacy, security, civil liberties and social justice.

These new location technologies share three key features: they can pinpoint coordinates, they can do so continuously and they can do so in real-time. This means that people using these technologies can potentially have their geographic position and travels traced anytime or all the time. What is more, the record of all these travels and habits may be stored and even shared by other parties for significant lengths of time.

Other technologies such as closed-circuit television (CCTV) and radio frequency identification (RFID) also yield information about the locations of people and goods, but are not considered in this report because they cannot track locations in a continuous fashion or in real-time. Tracking accurately, continuously and in real-time adds a new dimension to data collection that already includes isolated, historical information about the locations of people and things. This report focuses on aspects of data collection particular to location technologies and considers their implications.

We describe and consider a selection of increasingly relevant location technologies in this report. Emergency services, for example, use Enhanced 911's Cell ID (or Cell of Origin) systems to home in on caller locations. This service may be further enhanced with Global Positioning Systems (GPS). In addition to safety applications, separate but related systems can enable commercial uses of these technologies that provide billing, information, tracking and advertising applications.

Locations technologies do have weaknesses: they are unusable in buildings or underground, unless they are used in tandem with other technologies. This said, they may yet be developed in several different ways that are currently only at the design or testing stage. The forms that these technologies will take can only resolve once the market for location technologies becomes more established.

Current forecasts suggest that location-based service (LBS) markets are likely to grow significantly in the next few years. Some indicators hint at an annual rate as high as 80 percent, for some markets, while other forecasts caution that growth may be more gradual. A key impulse for market growth in the U.S. is the E-911 initiative, but this is likely to grow more slowly and patchily in Canada. Lawful access to personal communications is another push-factor as is fleet tracking performed by various business and public

sector services that wish to monitor drivers and vehicles in transit. Impediments to market growth in Canada include uncertainty about developments in the U.S., prohibitive deployment costs, piece-meal development and the sheer complexity of implementing these systems.

Once these costly and complex systems are in place, we expect that wireless carriers and LBS providers will be proactive in anticipating and addressing issues concerning the collection, use and disclosure of personal data. At the same time, businesses may be reluctant to offer assurances about data security because ensuring data security is an enormous, costly and never-ending task.

Many of the big questions about personal data have already been asked of other technologies, but location technologies raise new questions. Warehousing data and data mining are examples of concerns that already exist but so far there are no examples of the concerns that location data will add. It is precisely because we can only speculate about these new concerns, that we must try to anticipate them. Many of the obvious and the incremental changes introduced by location technologies are likely to be significant during the long-term.

Location-based advertising is an example of an LBS practice that raises new concerns. It is already considered intrusive in countries where it occurs extensively. Because many cellphone users in Canada are alert to privacy issues, companies are likely to be cautious about what third-party uses they permit. They will likely adopt an opt-in, rather than internet-style opt-out, method of consumer consent. The vulnerability of communications networks, especially those related to wireless infrastructure, is another serious concern for LBS. Compromised data security is a real issue. Rewards for fraudulent use are high and a number of cautionary tales are already well-known. Whether or not these concerns will translate into stronger legal measures is unclear.

Location technologies have special social significance because so many interactions now involve action at a distance, and they are interactions typically facilitated by new communications media. LBS enables comprehensive surveillance practices that are designed for the purposes of influence, management, care and control to monitor any number of individuals or groups of individuals. In a highly mobile era, when capitalism is defined by its management of consumption, LBS make sense not only as conveniences but also as means of tracking, profiling and sorting different types of customers, travellers, workers, citizens and others.

Our interviews with contemporary analysts thus considered not only privacy concerns that LBS raise, but also concerns that link location data with demographic characteristics and past behaviours. This sweeping range of location data, from any number of particular systems, makes the everyday activities of prolific numbers of people and groups of persons more visible and legible on the information landscape. This report outlines some of the issues that will help define information politics in coming decades.

Chapter 1
Location Technologies and Mobile Persons

Although they are in the early stages of development and adoption, it is clear that location-based services and tracking technologies are finding some ready markets

There is nothing new, nor necessarily anything sinister, about wanting to know where others are at any given time. Parents may want to be sure their children are safe in the big city, trucking companies may wish to ensure that their drivers are taking breaks of sufficient length and emergency services may be able to do a better job if they can find accident victims whether or not they can speak clearly into a cellphone. New technologies make all these things possible, automatically, remotely and in real-time.

A combination of political, economic and cultural pressures has produced a quest for new technologies that can locate people and objects and track their movement from one place to another. The pressures include a shift towards a safety-and-security state in which risk management is a key motif, a desire to realize the potential profitability of integrated and accelerated forms of organisational management and a cultural commitment to efficiency, productivity, convenience and comfort. The new technologies are of various kinds, including **RFID** (Radio Frequency Identification), **GPS** (Global Positioning Satellite) and **Wi-Fi** (Wireless Fidelity).[1]

In this report, however, we identify a little more precisely what we call location technologies. Although we make reference to other kinds of tracking devices and systems, our primary focus is with technologies that meet three specific criteria. They must **pinpoint locations;** they must do so **continuously**, and they must do so **in real time**. So while RFID and Wi-Fi present related issues, only those services that can give coordinates by calculating the longitude and latitude of a person's position are the ones considered location technologies in the sense used here. They can point to the exact place where the person is, and communicate this in real time to other persons or agencies, on an ongoing uninterrupted basis.

Although they are in the early stages of development and adoption, it is clear that **location-based services (LBS)** and tracking technologies are finding some ready markets, from car-tracking for security to more mundane domestic situations involving parents and teenagers. MobileIQ, based in Pickering, Ontario, offers a service designed to deter car thieves and lower insurance rates. GPS is used with a tracking device installed in the car so that it can be continuously followed in real-time and the route can be traced on the computer screen at home or in the office. Speed, location and direction of travel are all revealed at regular 3-5 minute intervals.[2] One location technology application in the U.S., Teen Arrive Alive, allows parents of children with GPS-enabled cellphones to track on the internet where their children are, and how fast they are travelling, on the highway.[3] The system's founders have begun to talk about selling their product in Canada.

[1] See David Lyon, 2005. "Why where you are matters: mundane mobilities, transparent technologies and digital discrimination", unpublished paper.
[2] Cribb, Robert. 2005. "Car tracking: Useful tool also gives you the creeps", *The Toronto Star*, March 21, Available: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout Article_Type1&call_pageid=971358637177&c=Article&cid=1111359009544.
[3] Church, Jack. 2004. "Keeping tabs on teens, by cellphone", *Ottawa Citizen*, September 22, A3.

In a world of high mobility, where so many everyday social relationships are mediated technologically, such developments are unsurprising. The high rates of mobility are themselves technology-dependent, of course. They emerge from ease of travel by car, train, and plane. But communication while in transit was until a very few years ago limited to visiting fixed telephones on the street, in airports, in train stations or in highway service areas. Today, not only phone calls, but text messaging and email or internet services are available on portable wireless devices. Now people can constantly be in touch, even while in transit.

The convergence of mobile computing devices has thus been greeted by many as an effective solution to perceived problems of a mobile society and as a great benefit to their users. This type of technology is culturally valued by different segments of the population. The obvious benefits of wireless and location-based technologies include safety applications that tend to take the lead in this field: **enhanced emergency wireless phone services (E-911)** is an example. Yet these benefits include many other applications like fleet tracking, product tracking, port security, parental control, law enforcement, mapping services and use by correctional facilities.

Put thus, the new technologies seem to support mobile lifestyles and to facilitate communication while on the move. At the same time, constant availability to others also means that personal information is flowing; these data may permit others to know where identifiable individuals are, in real time. Locational information (where you are, when) is valuable to some parties. Issues of **privacy** may be raised by this because some people may object to others knowing where they are. Beyond this, however, is the fact that location data may be of interest to other parties, such as insurance companies, police and marketing agencies, who may use them for more systematic tracking purposes.

Location technologies introduce new challenges with respect to privacy policy and law. For instance, how does consent operate when one is in a continuous circuit? Should consent be given only once, when signing up to use the cellphone, when the user is to be tracked every moment thereafter? Significantly, location information may be combined with other data to create profiles with yet another dimension, place, added to the previously existing mix. The parallels with already existing surveillance based on neighbourhood or on virtual movement on the internet suggest that such data will indeed be valuable. While parental tracking of teenagers may raise only privacy issues, important though they may turn out to be, commercial and law enforcement use of such data could well be significant for social sorting. The other, already existing, data are used to enable discrimination and differential treatment for different categories of persons and location data could well add one more dimension to the same processes.

Our findings show that mobile computing devices are becoming increasingly important within a context of growing technological convergence and rapidly rising availability of tracking technologies such as global positioning system (GPS) satellites. These factors raise important questions of how such converging technologies and ubiquitous networking will permit tracking of all kinds of users including employees, citizens, travellers

and consumers[4], plus two other significant categories, offenders and children. This report focuses mainly on consumer applications, although our findings have implications for other uses.

It is important to note that mobile computing devices such as **personal digital assistants (PDAs)**, cellphones and laptops and communication services such as Bluetooth, GPS networks and wireless **hotspots** are not necessarily considered tracking technologies by their designers and marketers. But because such devices and services are being integrated with a view to increased convenience and efficiency with location-based services (LBS) their tracking capacities have to be considered and assessed.

Location-based services (LBS) are one of the current applications being invested in, researched and implemented in Canada. The telecommunication industry intends to use LBS in order to improve public safety through an E-911 initiative, aid law enforcement through a lawful access initiative and develop LBS commercial applications for efficient mapping and directory services. In Canada, LBS are currently being used for fleet management, protection of goods and shipping management.

The perils of forecasting

There are other possibilities on the horizon, however, not all of which yet fit the location technology definition. The well-known inventor, Steve Wozniak, is actively designing cheap ways to keep track of things in a primarily domestic environment via his Wheels of Zeus investment[5], which would bring such services right into the home. In a local range of around three kilometres, he proposes a networked GPS system. Knowing the whereabouts of his pets was apparently his motivation, but the principle could be applied to elderly relatives as well. The positive benefits of such systems are palpable, but they could also be construed as potentially invasive.

Even more invasive, from the perspective of some, are proposals and even prototypes of tracking technologies that are implanted under the skin by means of a simple injection. Rather than remaining unsure whether or not the absent-minded granny is wearing her tracking device, the chance is offered to connect it permanently and invisibly with her person. Applied Digital's VeriChip which makes one of the best-known applications is, for example, in the process of acquiring BC-based Canadian location technology company eXI.[6] Once a RFID chip the size of a rice grain is implanted, the person's body is constantly traceable within a certain range, for better or worse. Coupled

[4] The four categories of worker, traveler, consumer and citizen are used within the Surveillance Project's 'Globalization of Personal Data' research project.

[5] ThHiltzik, Michael. 2004. 'Woz goes wireless', *Technology Review*, vol. 107, no. 4, May, pp. 42-45.

[6] "eXI'S Shareholders vote in favour of proposed acquisition by Applied Digital's VeriChip", 2005, *CNW Group*, March 14, Available: www.canadanewswire.ca/en/releases/archive/March2005/14/c4589.html

with GPS, however, this could become a powerful form of location technology.

We could continue, but the report would then become merely speculative. This report, however, is taken up primarily with what is actually happening in Canada, and to a certain extent elsewhere, in the realm of already existing location technologies. Technological forecasting is a notoriously problematic enterprise for many reasons.[7] This does not always stop people from hazarding forecasts, especially if they have a vested interest in self-fulfilling prophecies, but it will stop us. The main point of this report is not technological. It has to do with the social aspects of what these technologies enable – the processing of location data as personal data.

This means that our priorities as a research group are neither to sell the devices and their associated software and systems, nor to predict what the market will look like in a year's time, still less a decade's time. Our priority is to indicate what peculiar social, political, legal, and ethical challenges are presented by location technologies, understood as devices that can pinpoint continuously and in real-time people's locations. Companies will come and go, inventions will be hailed and will fail, users will construe and use certain devices quite differently from the ways in which they were dreamed up and designed. But within this volatility and flux, location technologies appear to be becoming increasingly important. So what are the main things to bear in mind?

New Technologies: New Issues

Although the issues raised by location technologies are not entirely new nor produced by the technologies themselves, several issues are highlighted by the advent of what have to be thought of as tracking devices. Such issues range from the misuse of the data to their vulnerability and lack of adequate protection, and the growing complacency surrounding their use. Some may be construed as privacy issues while others go well beyond this to questions of power and trust in contemporary culture.

Concerns about the misuse of location data are of more than one sort. One conern is that, with the integrated usage of mobile computing devices, location tracking devices and communication networks, there is potential for abuse of such technology through surreptitious or unwarranted tracking of the user. While forms of stalking may spring to mind, other more prosaic misuses may occur when tracking devices are used to regulate users. The case of Acme car rental agency, Connecticut, illustrates this well. Renters found that they were charged additional fees for speeding in Acme cars. The possibility that they might be fined by the agency had not been disclosed to customers. The offenders were caught through the use of on-

[7] Daniel Bell's classic *The coming of post-industrial society: A venture in social forecasting* (New York, 1971) took these difficulties very seriously but even he has now been shown to be mistaken about a number of aspects of his 'forecast.'

board GPS systems.[8] Consumer groups successfully fought this and won on the grounds that the rental company had no ability to charge fines when no damage had been done to them.

Another important concern under the misuse heading is that, in addition to current personal information that has been collected from a user, the use of location-based technology in tandem with wireless technology now adds geographical location information to the catalogue of personal information acquired. Marketing companies are especially interested in such data, indeed with increasing strategic integration between marketing and security agencies, these data may well turn out to have considerable added value. After the 2005 data breach at Choicepoint in which a con artist gained access to the company's data warehouse through conventional request, it once again appeared to many that security breaches were still a risk, even in a very large well-established company such as Choicepoint.

The problem is that companies such as Choicepoint are extremely interested in all kinds of personal data, including locations. In the U.S., Choicepoint can actually obtain certain kinds of information that it is illegal for government departments to monitor. And it is precisely the capacity to combine these data with others to create detailed profiles for which Choicepoint has justly become famous – or notorious, depending on your viewpoint. Law enforcement and security authorities seek these data from Choicepoint and similar companies, on a routine basis.[9]

Other concerns include the vulnerability of the new location technologies to unauthorized interception. A number of critics complain that mobile computing devices possess weak communications security.[10] Currently, wireless communication is poorly encrypted, leading many users to wonder how vulnerable they really are to hackers and war-drivers. When mobile computing devices are partnered with GPS and mobile technology, a user's location and the context they are working within in real-time can become vulnerable to penetration alongside their communication content.[11]

Because location data relating to people can be very valuable, weak security combined with technological convergence is likely to lead to an increased distrust in the wireless industry's ability to protect a user's personal information. There already exists a widespread belief that the industry that provides such services is complacent regarding unwarranted surveillance, collection and use of such personal information.[12] In addition, Canada's federal private sector privacy legislation, the **Personal Information Protection and Electronic Documents Act (PIPEDA)**, is viewed by many in the telecommunications industry as

[8] Lemos, Robert. 2001. "State puts brakes on GPS speeding fines", *News.com*, July 2, Available: http://news.com.com/2100-1040-269388.html?legacy=cnet.
[9] Harris, Shane. 2004. "Private Eye", *Govexec.com*, March 16, Available: http://www.govexec.com/features/0304/0304s1.htm.
[10] Patten, Brad. 2000. "Pay attention to your security with wireless networks" *The Business Journal of Jacksonville*, November 29; Schneier, Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World*, New York: Wiley Computer Publishing.
[11] Crowe, David. 2004. "Wi-Fi, Wi-Max: Taking wireless security seriously", *Wireless Telecom*, Issue 3.
[12] Cavoukian, Ann. "Privacy Protection is Good Business" Speeches 2000-2005, Available: www.ipc.on.ca/speeches/.

being vague (as some of our interviewees made very clear) with numerous grey areas, and a relative lack of enforceability.

In the longer term, it must be observed that a generational factor will play a part in determining the extent to which location technologies are used and regulated. There is evidence that people under 35 tend to be less concerned about the tracking and surveillance possibilities of location technologies than older age groups. A Canadian study found that younger people are little concerned with personal privacy protection, except to avoid identity theft. The tactic of creating fake personae used in this case is of little use when it comes to location technologies and tracking devices.[13] By default it is likely that the benefits of the new technologies will be seen by younger people as paramount and the negative aspects as less significant.

The Scope of this Study

The purpose of this report is to draw attention to some current concerns about tracking different groups using location technologies and mobile computing devices. It also offers a guide to the ways in which such convergence is affecting the wireless landscape and the various applications, current and future capabilities, current industry drivers and growth. Attention is paid to what manufacturers and service providers of such technology are doing to ensure compliance with privacy legislation (PIPEDA) and privacy controls/expectations. It also provides an assessment of whether such corporate strategy resonates with public expectations of such services.

This report also assesses the social significance of surveillance practices along with some informed speculation about what directions the industry and technology are taking and where problems, discourse and further concerns may arise. Again, the distinction is drawn between perceived privacy issues and issues that go beyond this to create situations vulnerable to social sorting and digital discrimination. Both kinds of issues are raised by location technologies and it is a mistake to minimize the significance of either.

The writing of this report was made possible by funding from the Office of the Privacy Commissioner of Canada and draws on various resources such as interviews with leading experts, including technologists, industry association representatives as well as service provider representatives and industry project leaders. The interviews took place early in 2005, mainly in Ontario, and explored in open-ended fashion the current state of the market and concerns about location technologies, privacy and security, within the Canadian landscape. The interviews provide some background to

[13] Media Awareness Network, "Young Canadians in a Wireless World" Phase Two Findings: Privacy, Intimacy, Security and Ethical Behaviour", Available: www.media-awareness.ca/english/special_initiatives/surveys/phas_two/upload/yccww_phase_two_report.pdf/.

what is discussed, and are quoted at appropriate points throughout the report. Secondary information sources are also cited in the report, including books, industry websites, magazines, company privacy policies, surveys, and newspaper articles.

The structure of the report is as follows. Chapter 2 focuses on defining location technologies in terms of their technical capacities, discusses current applications and comments on where today's developments seem to be heading. Chapter 3 takes this further, looking at current location-based services (LBS) and what is actually happening in the field. Chapter 4 turns to issues of privacy and data security, at both a company and a popular level. Chapter 5 widens the lens angle to consider the cultural context in which location technologies operate, and how they contribute to the development of surveillance societies. Chapter 6 briefly summarises some possible policy directions and some areas for future research.

Chapter 2

Location Technology Defined and the Future of LBS

Over the last five years, location technology has turned an individual's current location information into a valuable commodity, improved organisational efficiency and provided another law enforcement and public safety tool. Where you are, does matter.

Knowing where persons are at any given moment, and being able to trace and track them has implications for privacy, civil liberties and social justice.

Location technology is unique because it allows one to seek out a geographical location device (receiver), in some cases with pinpoint accuracy.[14] These devices are typically connected in some way to an individual. This is why location technologies should be considered in relation to other means of gathering and processing personal data. Knowing where persons are at any given moment, and being able to trace and track them has implications for privacy, civil liberties and social justice.

For some deployments, locations can be tracked without the device making its whereabouts known first. Location technology is also unique because it allows for continuous and therefore real-time tracking of a device. However, the commercial application of these capabilities has been viewed by many potential service providers and users as costly, invasive, unnecessary and/or extremely resource dependent. As a result, location technology is most commonly deployed either through a wireless handset or a network of cell sites or base stations. Location based services usually only exploit one or two of three techniques: Cell-ID or **Cell of Origin (COO)**, **Enhanced Observed Time Difference (E-OTD)** and GPS/Assisted GPS. These techniques, which will be described shortly, allow users to find information related to individuals's current or future locations.

Other tracking technologies, such as active radio frequency identification (RFID) tags, only provide location information based on the continued emission of a frequency from the tag that is then picked up by proximity to a configured reader. In the case of a closed-circuit television (CCTV) camera system, a person would have to actually appear on screen and stay within the camera's view in order to be tracked. Red-light cameras are only capable of capturing a "one-shot transaction"[15] similar to a record generated by a credit or loyalty card. Similarly, biometric and credit card technologies require a swipe or scan of a card or body part in order for data processing to translate the information acquired into location data. Therefore, most tracking technologies rely on a checking-in feature in order to track an item or individual. Even then tracking and acquiring location information about an individual or item is limited to the areas where such data can be collected.

It is worth noting here that the ability to track the location of human beings on the one hand, and other living things or objects on the other,

[14] Pinpoint accuracy is usually considered to be anything less the five metres, but is generally only utilized for military surveillance and tracking. There is currently no broad-based commercial service that exploits this type of accuracy.

presents new challenges with respect to privacy policy. Privacy legislation protects the information of individuals and not of items. Yet a device such as a cellphone can yield location information which may or may not correspond to the whereabouts of the individual presumed to be the user. This and related points will receive further attention in chapter 4.

Within this report, location technology is defined as an application that can provide continuous, real-time and accurate location information about an individual or item. Technologies which have been designed such that they need not always provide continuous tracking and accurate location information are included in our definition of location technology because these capabilities may still potentially be switched on. The location techniques which make these technologies operable are reviewed below.

Cell-ID or Cell of Origin (COO)

One of the most basic forms of location tracking techniques is known as Cell-ID or Cell of Origin (COO). It uses a mobile-network operator to determine a mobile user's whereabouts through the identification of cell sites or base stations that are close by. Such a technique is not regarded as the most precise locator because it considers the location of the cell site to be the location of the user. Accuracy is, therefore, improved with an increase in the density of cell sites. Cell-ID or COO, which is most commonly used for emergency services and infrastructure, has been deployed in the United States during Phase 1 of the E-911 initiative.[16]

In urban centres, where cell sites are found in greater density, accuracy results are usually estimated between 50 and 250 metres. In more rural areas, accuracy can decrease to a radius of more than 20 kilometres, which makes the service unviable when precision accuracy is required.[17] To improve accuracy, Cell-ID or COO is generally used in conjunction with some other location technology such as Enhanced Observed Time Difference (EOTD) or Global Positioning Systems (GPS). However, Cell-ID or COO is a preferred basic technique because this technology requires no major adjustments to the mobile network or mobile terminal, which makes it easily deployable and relatively affordable. It can also identify the location of a cell site in approximately three seconds which is very quick.

Enhanced Observed Time Difference (E-OTD)

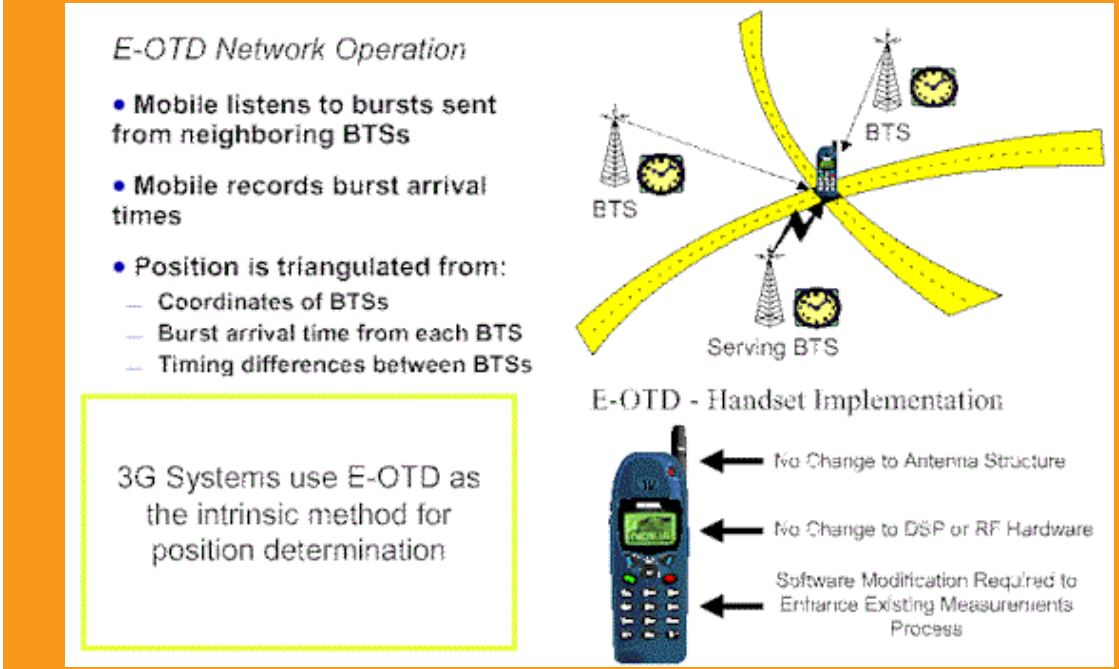
E-OTD technology was developed by Cambridge Position Systems. This technique operates through cell sites as well but measures how long it takes radio waves from two different cell sites to reach a user's mobile terminal. It

[16] In 1996 in the U.S., the Federal Communications Commission (FCC) developed a mandatory initiative to address the improvement of communication and response times amongst emergency service personnel and any wireless caller in distress or requesting emergency help.
[17] *Wireless Location Services for Telematics have yet to Thrive*. 2002. Technology Analysis, Gartner Inc., July 23, pg. 3.

then locates that terminal using a triangulation technique that measures the radial distance or direction of a received signal from two or three different points. Once a signal from two or three cell sites is received, the E-OTD software enabled mobile and the triangulation measurement of the cell sites are calculated based on the different times it takes the signal to arrive at the receivers once it leaves the mobile handset (see figure 1). The differences in time are combined to produce intersecting lines from which the location is estimated.

Theoretically, E-OTD can provide accuracy of between 30 and 50 metres, but real-world tests have yielded less accurate measurements of between 50 and 125 metres. Regardless, E-OTD is a relatively accurate location measurement technique. E-OTD requires an upgrade to the mobile-network infrastructure and requires the loading of network software within cell sites to ensure compatibility; this can mean the deployment of new cell sites altogether. Response time of location measurements is also slower than Cell-ID or COO, typically identifying a location after five seconds.[18] A very similar technique known as Observed Time Difference of Arrival (OTDOA) has been and will continue to be deployed to service third-generation (3G) mobile networks for commercial use.

Figure 1: E-OTD



Source: Raddcomm wireless consulting services

[18] Prasad, Maneesh. "Location Based Services." *GIS Development*, Retrieved: January 21, 2005, from www.gisdevelopment.net/technology.lbs.techlbs003pf.htm, pg. 2

GPS and Assisted-GPS

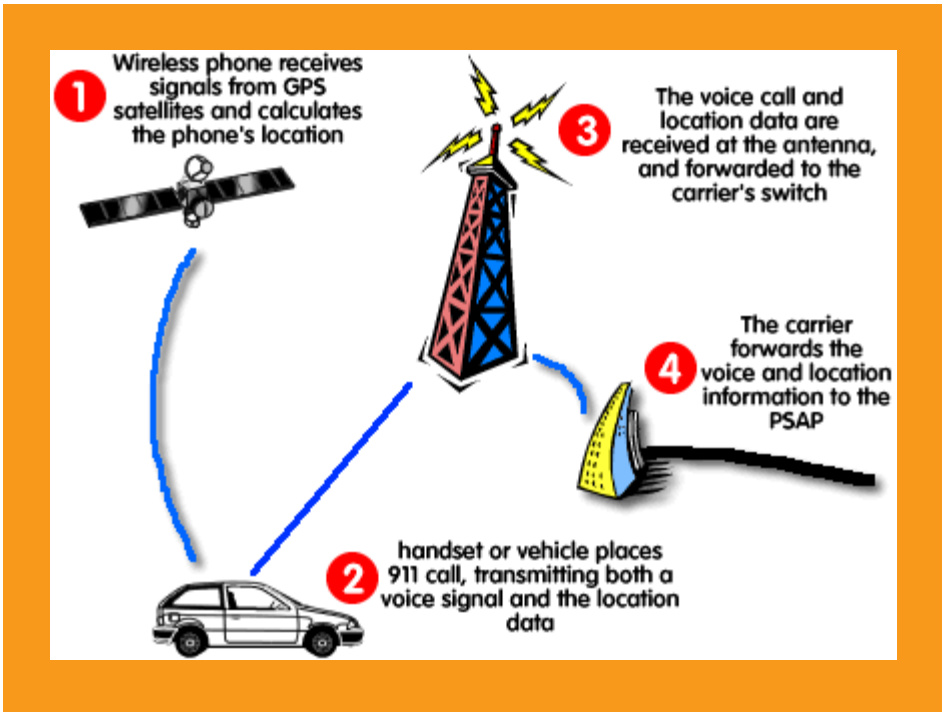
The Global Positioning System (GPS) is a worldwide satellite navigational system made up of satellites orbiting Earth and their corresponding receivers on the ground (see figure 2). These satellites orbit Earth at approximately 19 000 kilometres above the surface and make two complete orbits every 24 hours.[19] GPS was first developed in 1957 as a receiver to listen for the Russian satellite, Sputnik. Since then, it has been transformed from a technology used solely for military purposes, such as searching for enemy communications and helping in military navigation, to a commercially viable, real-time, multi-satellite network. It is known as GPS or the Global Positioning Satellite System (GPSS). It is most commonly defined as a technology that is used to assess the position of compatible receiver units (such as cell sites) using satellites to provide 24-hour positioning information regardless of weather. Like E-OTD, it determines position through the method of triangulation. Prior to May 2000, GPS location accuracy capabilities were controlled by the U.S. government, which diluted precision to no less than 100 metres. This dilution of precision has since been turned off and accuracy has been increased to within five metres.[20] However, as mentioned by a representative from a Canadian wireless vendor, despite the government's relinquishing of accuracy control "industry has still not caught up, preferring at this time to continue to use land-based wireless location signals."[21]

The opportunity to enhance location accuracy was the catalyst for turning GPS into a commercial location technique known as assisted-GPS. This technique combines the capabilities of GPS with wireless-network capabilities. Assisted-GPS requires that three or more satellites are in the line-of-sight of a user's mobile handset that must be equipped with a compatible chip. Assisted-GPS then links to the terrestrial-based system of cell-sites to help speed the process of connecting the handset to the GPS satellites and calculating position (see figure 3).[22] However, maintaining a line of sight becomes increasingly difficult in urban areas rendering it unreliable or ineffective, particularly inside buildings or underground. Assisted-GPS can be accurate within ten metres but is expensive for the end-user as it requires a GPS-equipped handset.[23] It also requires wide-ranging upgrades to network infrastructure as well as the deployment of new mobile terminals. Integrating the technology into mobile terminals can cost anywhere from $25 to $50 per terminal. Although far less costly than integrating full GPS capability because it relies on cell-site triangulation, Assisted-GPS can still increase the total cost of materials.[24]

---

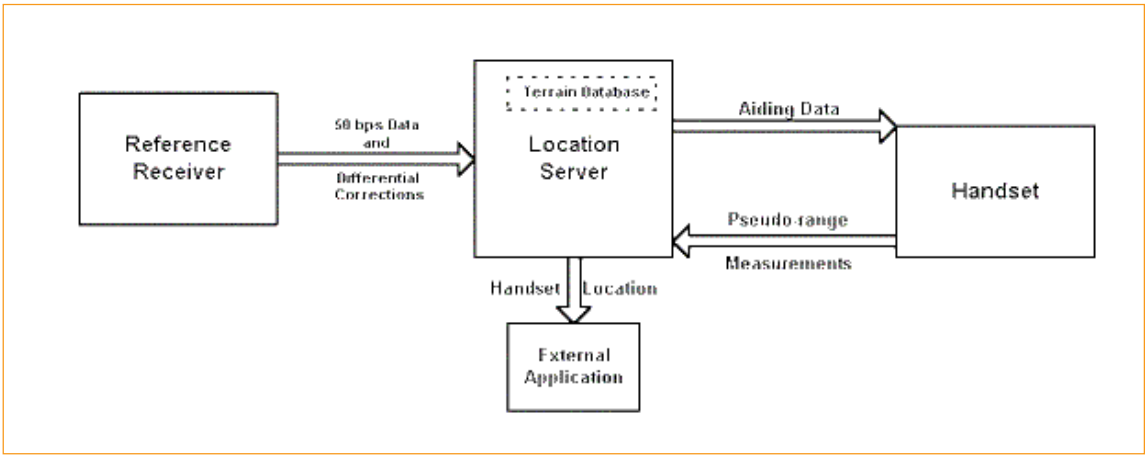
[19] "What is GPS?" *Webopedia*, Retrieved: January 1, 2005, from http://www.webopedia.com/TERM/G/GPS.html.
[20] *Gartner's Glossary of Wireless Mobile Terms: 2002 Update*. 2002. Strategic Analysis Report, Gartner Inc., June 12, pg. 14.
[21] Interview, February 23, 2005.
[22] Blackwell, Gerry. 2001. "Location, location, location." *Wireless Telecom,* Vol. 19, No. 3, pg. 43.
[23] Prasad, Maneesh. "Location Based Services." *GIS Development*, Retrieved: January 21, 2005, from www.gisdevelopment.net/technology.lbs.techlbs003pf.htm, pg. 2.
[24] *Wireless Location Services for Telematics have yet to Thrive*, 2002. Technology Analysis, Gartner Inc., July 23, pg. 3.

Figure 2: Assisted GPS



Source: Raddcomm wireless consulting services

Figure 3: Assisted GPD Data Flow



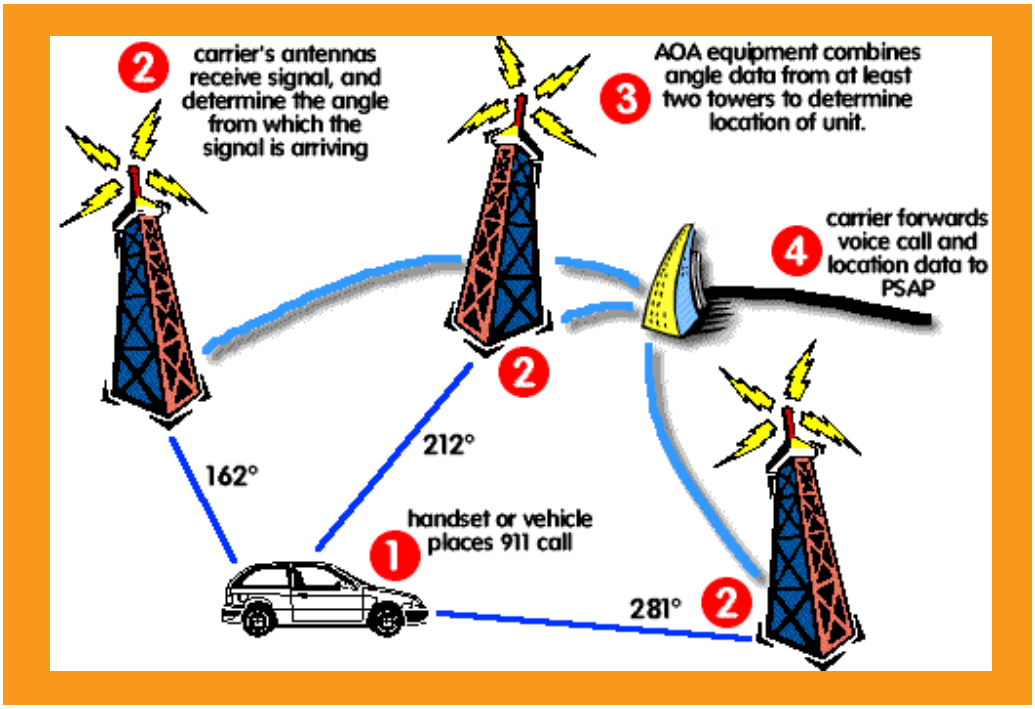
Source: Raddcomm wireless consulting services

Some additional location tracking techniques include the following:

Time of Arrival (TOA) is a method of locating a wireless caller by calculating the time of arrival of the signal from the mobile to more than one base station. It requires synchronization of the cellular network using GPS at each cell-site, which is outfitted with location measurement units (LMUs). Measuring the signal from the mobile phone will determine the user's position. Although TOA is more accurate than Cell-ID or COO, the implementation of all of the required LMUs is very expensive. The cost and overhaul of a network that is required to implement TOA may be disproportionate in relation to the resulting accuracy enhancement, unless service providers supply their own overlay service to attach to a network.

Angle of Arrival (AOA) is a method that calculates the direction from which the caller's signal is arriving through the deployment of antennas within each cell-site (see figure 4). Although more accurate than Cell-ID or COO, without a service provider with overlay capabilities, it too can be quite costly to configure and outfit the various cell-sites used to operate the service.

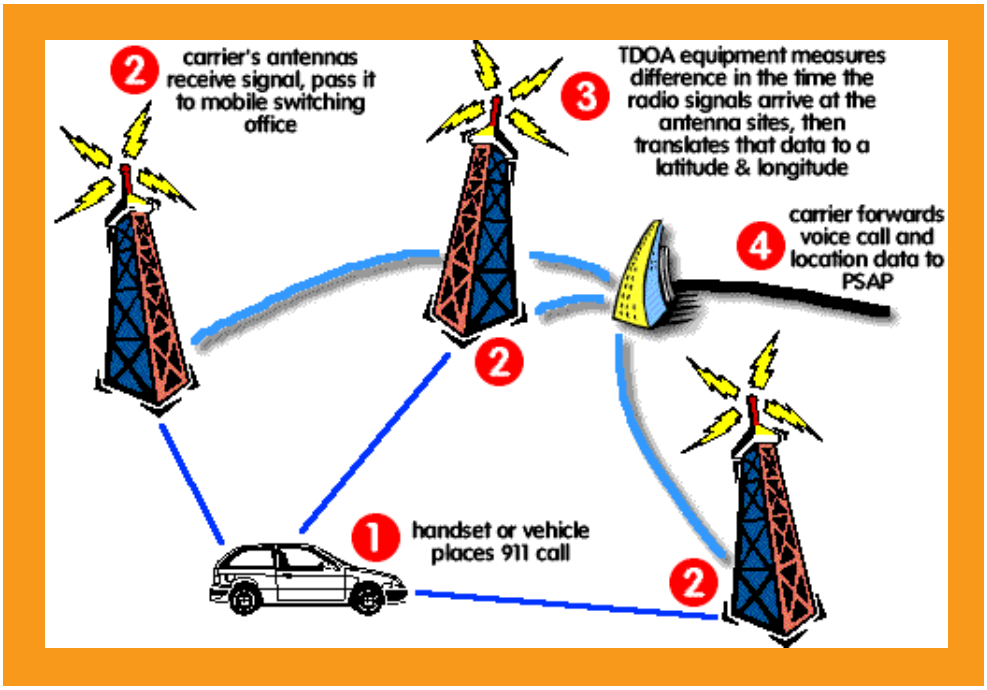
Figure 4: Angle of Arrival



Source: Raddcomm wireless consulting services

Time Difference of Arrival (TDOA) is also a method that uses antennas to calculate the location of a wireless caller (see figure 5). Because these antennas are found at different distances from where the caller may be, the signal that arrives from the caller will arrive at slightly different times. Using at least three different signal times from three separate antennas, the location of the caller is then calculated. Again, like TOA and AOA, without a service provider's overlay infrastructure, the cost of outfitting and configuring the network outweighs the limited accuracy enhancement that this technique provides, particularly due to its long response time of ten seconds.[25]

FIgure 5: Time Difference of Arrival



Source: Raddcomm wireless consulting services

[25] Prasad, Maneesh. "Location Based Services." *GIS Development*, Retrieved: January 21, 2005, from www.gisdevelopment.net/technology.lbs.techlbs003pf.htm, pg. 2.

Location-based Services

Location-based Services (LBS) include all of the above techniques and technologies in a category of services that enhance the end-user application for mobile telephones and devices. In other words, "they provide the ability to find the geographical location of the mobile device and provide services based on this location information."[26] Generally, it is forecast that LBS will be based on increasingly accurate technologies that will be deployed on a telecommunication carrier's infrastructure and in the handsets that are provided to the user.

Currently, LBS applications are separated into the following categories:[28]

Safety applications provide an automatic location of caller service that is connected directly to emergency telephone services so that a user may be provided with requested assistance based on their location. Some examples include the on-board vehicle emergency assistance service provided by On-Star or the mandated E-911 initiative in the U.S. that requires all public agencies that respond to 911 emergency calls to work with telephone companies and the wireless industry to generate

Elements of a Service

In order for LBS to be provided to an individual, four key events must occur:

1. Location technology information must be placed through a reference system such as a mobile network or global positioning system (GPS) and then embedded in the network or mobile network.

2. Servers must convert this location data from the network into geographical coordinates of longitude and latitude. This is not done if using GPS.

3. Geographical databases must then provide location servers with geographical, predetermined data to derive longitude and latitude from the handset position.

4. Location applications must then provide the particular services (e.g. real-time, local traffic information). The caller's geographical coordinates are translated as input, while using location content databases, and then the requested information is provided.[27]

[26] Prasad, Maneesh. "Location Based Services." *GIS Development*, Retrieved: January 21, 2005, from www.gisdevelopment.net/technology.lbs.techlbs003pf.htm, pg. 1.
[27] *User location data will give MNOs an edge*. 2001. TG-14-0934, Gartner Inc. July 17, Pg. 1.
[28] *Gartner's Glossary of Wireless Mobile Terms: 2002 Update*. 2002. Strategic Analysis Report, Gartner Inc., June 12, pg. 18.

a broad-based emergency services network of location-finding technology.

Billing applications provide automatic payment services, so a user can receive discounts on services such as calls made based on their location.

Information applications provide information actively requested by the user based on their current location. Some examples include sending the user requested directions to desired restaurants or events and/or location-based traffic updates while a user is on the road.

Tracking applications provide services with the use of monitors and embedded tracking devices that can track a number of items or people to ensure safety, business efficiency and accountability. Generally this type of application is used by organisations that must oversee large fleets of vehicles (such as taxis or trucks) or by those responsible for the safety of other individuals. However, this type of tracking is very flexible. Its application has many possibilities such as the tagging of golf balls with satellite transmitters to track a player's performance.

Advertisement applications provide location-sensitive pages through advertising services to a user's mobile device. For example, a user could be provided with discount coupons if walking by a corresponding store or restaurant. It should be noted that unlike the case of information services, the delivery of advertisements at any specific point in time is triggered by the organisation and not the individual. This holds true whether advertising of a particular kind has been requested by a given individual, or whether unsolicited advertisements are delivered in the form of "spam." These issues will receive closer attention in chapter 4.

Associated Technologies, Ubiquitous Networking and the Future

Although location technology and LBS have a lot to offer a wireless mobile user (and the better the technology gets, the more uses people find for it) they still suffer from a number of potential limitations. However, several technologies have appeared on the market which may be able to compensate for weaknesses in current location technology functions.

One weakness associated with most location technologies is that once a mobile user moves inside a building or goes underground, use of any LBS becomes virtually impossible. As previously indicated, a user's mobile device must maintain a line-of-sight with either the cell sites or satellites in the user's area. When entering into a building or going underground, technology such as Bluetooth or Wireless Fidelity (Wi-Fi) could pick up where location

technology leaves off by providing integrated, world-wide, short-range radio specification focused on continued communication between devices and computers indoors or in urban areas. This includes communication between an LBS provider's network and Bluetooth or a Wi-Fi-enabled handset. However, such complementary technology requires dense and fixed infrastructure which would best be used as hotspots,[29] "busy areas where mobile device owners will congregate."[30]

The integration between LBS and Bluetooth or Wi-Fi could be of greatest benefit to emergency response teams such as fire fighters. Fire fighters could be continuously tracked even when inside a burning building if complimentary receivers were connected to external location-based receivers.[31] At the same time, the use of location technologies by firefighters and numerous other categories of workers raise new concerns with respect to employer/employee relations and workplace conditions. Some of these will receive attention in chapter 4.

Short Message Service (SMS) is another technology that allows for up to 160 characters of text or 140 bytes of information to be sent and received through a mobile device. To reduce reliance and cost on some of the more expensive and less accurate location technologies such as TOA or AOA, SMS can be coupled with basic Cell-ID or GPS receivers to transmit location information to the user or host and back again. Therefore, SMS allows for one of the most cost-efficient means of communication of location-specific information such as receiving the latest traffic reports or directions to the nearest restaurant. Combining SMS with GPS ensures a high level of accuracy and convenience and is therefore most frequently used by those tracking vehicles and transporting prisoners. SMS and GPS two-way communication possibilities could also mean that service providers could offer additional "in-vehicle services, such as traffic-flow overlays and location-specific information regarding the whereabouts of the nearest filling stations, restaurants or hospitals."[32]

A high number of **peripherals** are also providing better presentation, convenience and reliability for location-based services. As mentioned in the introduction to this report, Steve Wozniak, inventor of the Apple Computer, is investing in networked GPS systems, through his new company Wheels of Zeus. They will allow users to connect inexpensive and unobtrusive GPS devices to anything marked as important in their daily lives such as children, pets, elderly relatives, cars or "anything else that could end up in an unsafe, inappropriate, or unauthorized place."[33] This technology would keep track of such individuals or items through the use of a wide range of wireless applications such as personal

[29] The definition of a hotspot is "A specific geographic location in which an access point provides public wireless broadband network services to mobile visitors through a wireless local-area network. Hotspots are often located in heavily populated places such as airports, train stations, libraries, marinas, conventions centers and hotels. Hotspots typically have a short range of access." "What is a hotspot", Webopedia, http://isp.webopedia.com/TERM/h/hotspot.html, Retrieved: March 10, 2005.

[30] *Mobile Location Services: No Mass Market in Europe Until 2007*, 2001. Gartner Inc., July 9.

[31] Pfeiffer, Eric W. 2005. "WhereWare", *Technology Review*, Retrieved: January 26, 2005, from www.technologyreview.com/articles/03/09/pfeiffer0903.asp?p=0, pg. 2.

[32] "Wireless City showcases Calgary tech", 2004. *Backspace Magazine*, Nov/Dec.

[33] Hilzik, Michael A. 2004. 'Woz goes wireless', *Technology Review*, vol. 107, no. 4, May, pg. 43.

digital assistants (PDAs), mobile phones, personal computers and home phones through an alert-based system. By using a low-speed, low-power and thus a low-cost network that Wozniak calls "wOzNet," it would connect local hotspots, which have an approximate range of three kilometres, to the user's home network of receivers.[34] The user sets the parameters and receives alerts when individuals or items breach a specified area.

Various other companies such as Applied Digital Solutions (ADS) and Pro Tech Monitoring, both based in Tampa, Florida, provide more sophisticated LBS through a pager-like or watch-like device (rather than through a basic base-station model) that can be attached to a person or animal that is expected to remain in a particular area.[35] All of these user-enabled services have set the stage for the future possibility of ubiquitous networking that allows all program applications via LBS technologies and peripherals to follow individuals wherever they go. Although not yet deployed on a regional, national or international scale, if compatibility and cost issues can be reduced, users can expect to be provided with wider-reaching, more accurate, more efficient, and increasingly individualized services. These points are important, since the blending of LBS into the routines of daily life may make consumers less guarded with respect to potential threats to the privacy and security of their personal information. Furthermore, greater commercial control over the consumer's environment and an enhanced ability to identify social groupings in the form of niche markets, will inevitably have significant social consequences unlikely to be anticipated by users. These points will be elaborated in chapters 4 and 5.

Many industry experts and technicians expect that location technology devices will soon be miniaturized to such an extent that they may be built into belts, shoes and even clothing. LBS devices have also changed shape, and now offer alternatives to mobile phone chip or wristwatch models. These include human chip implants that can track human targets of kidnapping, and specially moulded devices that may be camouflaged within a certain area of a vehicle to avoid tampering. Wherify is an American product and service provider that is currently considering the development of a flat version of its tracking device to be slipped into a stack of banknotes during a robbery. They are also in the process of launching the world's first business card-sized, GPS-enabled mobile phone, the Wherifone G550 Locator Phone.

More inventive services, like the commercial-based applications mentioned above, will expand the uses of LBS. Service providers have even imagined the launch of a buddy locating service that can alert users when friends or colleagues are within a certain distance from them.[36]

[34] Hilzik, Michael A. 2004. 'Woz goes wireless', *Technology Review*, vol. 107, no. 4, May, pg. 43.
[35] "Something to watch over you." 2002. *Economist.com,* March 13, Retrieved: January 24, 2005, from www.economist.com/PrinterFriendly.cfm?Story_ID=1280634.
[36] Blackwell, Gerry. 2001. "Location, location, location." *Wireless Telecom,* Vol. 19, No. 3, pg. 46.

Entirely different technologies may also come to market that will continue to enhance LBS or even take its place. One example that is getting attention from the Ottawa Wireless Research Alliance is the development of a radio technology known as Software Defined Radio (SDR), which can potentially configure a wireless device to work with any communications system. SDR "will allow a single device to adapt to different communication environments and systems by selecting a software program that will emulate the appropriate protocol and frequency needs for the communications link, empowering any location technology that is also integrated into such a capability."[37] Although still in the early stages of development and application, SDR has gained popularity within the military, public safety and commercial wireless sectors.

The Economist's Technology Quarterly observes that it is "naïve to imagine that the global reach of the internet and advancing technology would make geography irrelevant."[38] In fact, precisely the opposite appears to be the case. Knowing the precise location of persons or objects is now a major preoccupation of marketers, employers, travellers, parents and others. While growing at different rates of use, and employing different techniques and infrastructures, LBS are increasingly being looked to for a wide range of commercial, legal and governmental applications. While the future of LBS are difficult to predict, the next chapter highlights the economic and political factors most likely to condition their growth in Canada. Chapters 4 and 5 will explore related issues pertaining to consumer habits, conditions in the workplace, governmental uses of location technologies, and evolving perceptions of privacy.

[37] "Software Defined Radio (SDR)." 2005. *OWRA/IEEE COMSOC/NCIT/CRC Seminar Day*, January 14, Ottawa.
[38] "The revenge of geography." 2003. *The Economist.com*, March 13, Retrieved: January 24, 2005, from www.economist.com PrinterFriendly.clm?Story_ID=1620794.

Chapter 3

LBS Market Forecasts, Drivers and Impediments to Growth

Leading commentators predict that mobile and location-based communication services will soon exist everywhere in the world's rich nations. Others are more sanguine, suggesting that a number of hurdles will have to be crossed before significant use of LBS becomes evident. The situation in Canada is unclear at present, so caution is called for in assessing the forecasts. In an interview with a wireless association member, the future of LBS was discussed in terms of its current and potential popularity. He remarked that "not only do we live in what I like to call a communications era, we really live in a situation now, and not only just in Canada but globally, where you can classify and expect anywhere, anytime communications. . .. People are probably going to expect that they'll be able to find out the information that they're looking for based on where they are."[39] Expectations such as this may be weighed in part against relevant marketing forecasts and also in light of precedents concerning early deployments of LBS in other parts of the world.

World Market Forecasts

- Strategis Group asserts LBS market size will be $3.9 billion by 2004 in the U.S.[40]
- Allied Business Intelligence Inc. (ABI) estimates world LBS revenues growing from approximately $1 billion in 2000 to over $40 billion in 2006, representing a compound annual average growth rate of 81 percent.[41]
- In-Stat Group has forecasted that worldwide revenues will reach $13.3 billion by 2005 and a 514 percent compound annual growth rate between 2001 and 2005.[42]
- Ovum, a U.K.-based consulting firm, predicted in 2000 that LBS would create $420 billion in revenues by 2006 worldwide, "including $10 billion in mobile commerce transactions powered by automatic location determination and $4.5 billion for advertising over mobile terminals using location as a trigger." However, Ovum also warns that LBS has the potential to become transparent and to no longer act as a market differentiator after it passes its initial "golden age."[43]
- Strategis Group suggests that, within the Asia-Pacific market, wireless internet users will increase from 20 million in 2000 to 216.3 million by 2007, and further suggests that a wider market of wireless users may mean a broader-based market to promote add-on services such as LBS.[44]
- In 2001, Upinder Saini, Director of New Product Development at Rogers AT&T Wireless, even suggested that, "over the next four or five years, we can expect this to be a multi-million dollar – or even multi-billion dollar business."[45]
- IDC further reports that two-thirds of Americans want wireless LBS for safety and security applications and states this as the primary reason for wanting LBS.[46] Respondents to this survey suggest "they would even be willing to pay a premium to have location capabilities in their handsets or receive advertising on their handsets to reduce or eliminate telematics service charges."[47]
- Less optimistic views have also been expressed. During a European Symposium on Mobile Technology, Gartner surveyed the 124 delegates regarding their potential use of location technology. 61 percent of respondents stated, "That they either didn't need location services or didn't know what role such service might play."[48]

[39] Interview, February 24, 2005.
[40] Prasad, Maneesh. "Location Based Services." *GIS Development*, Retrieved: January 21, 2005, from www.gisdevelopment.net/technology.lbs.techlbs003pf.htm, pg. 1
[41] McKeefry, Hailey Lynn. 2004. "Location-Based Services Come of Age", *Mobilized Software*, Retrieved: March 3, 2005, from www.mobilizedsoftware.com/showArticle.jhtml?articlesId=18901516.
[42] Blackwell, Gerry. 2001. "Location, location, location." *Wireless Telecom,* Vol. 19, No. 3, pg. 40.
[43] Ibid. pg. 40
[44] Prasad, Maneesh, GIS Development, pg. 1.
[45] Blackwell, Gerry. 2001. "Location, location, location." *Wireless Telecom,* Vol. 19, No. 3, pg. 40.
[46] Ibid, pg. 1.
[47] Ibid, pg. 1.
[48] *European Symposium Mobile Technology Survey.* 2002. COM-14-9382, Gartner, Inc. January 22, pg. 2.

When viewed together, all of these forecasts and surveys demonstrate just how unknown the future will be for LBS's market growth and popularity on a worldwide scale. Although popularity and use have increased in particular regions, such as Japan, Korea and the U.S., they have not generated enough interest to classify LBS as a highly successful harbinger of a completely wireless service society. Michael Sheha, President of Networks in Motion, notes, "Every year we've heard that this is going to be the year for location-based services," leading many to now believe that LBS will only bring small, incremental amounts of revenue. Regardless of this fact, Sheha still believes that with several market drivers in motion LBS are bound to take root on a wider scale eventually.[49] Market forecasting is a notoriously uncertain art. Although there have been market drivers, which will be addressed below, that have aided in some growth, there are still various impediments keeping LBS from being deployed into every aspect of wireless communications.

Market Drivers and Potential Advantages

Location-based technologies and services have numerous potential advantages, which include a range of social and economic benefits. Charlie Trimble, President of Trimble Navigation Ltd., suggests that knowledge of position has tremendous benefits "in helping to feed the world, to provide more efficient commerce and therefore a better quality of life, to provide better safety and security."[50] However, advantages do not necessarily line up with initiatives underway that are bringing location technologies to the foreground.

One important driver to produce and deploy location technology is the E-911 initiative. In 1996 in the U.S., the Federal Communications Commission (FCC) developed a mandatory initiative to address the improvement of communication and response times amongst emergency service personnel and any wireless caller in distress or requesting emergency help. It requires that wireless carriers be able to pinpoint a mobile caller's telephone number, and that emergency dispatchers have access to this information. Relatively recent data show that calls for such an application are compelling. In the U.S. alone, 40 to 50 percent of all 911 calls now originate from mobile phones.[51] The National Emergency Number Association (NENA) in the U.S. estimates that 45 million of those calls were made on cellphones.[52] With numbers continuing to rise, carriers are now providing mobile users with services and enabled handsets. Similar action is being taken in Europe to introduce a continent-wide emergency response service known as E-112.

---

[49] McKeefry, Hailey Lynn. 2004. "Location-Based Services Come of Age", *Mobilized Software*, Retrieved: March 3, 2005, from www.mobilizedsoftware.com/showArticle.jhtml?articlesId=18901516.
[50] Tristram, Claire. 1999. "Has GPS lost its way?" *Technology Review*, Retrieved: February 7, 2005, from http://www.technologyreview.com/articles/99/07/tristram0799.asp?p=1, pg. 1.
[51] *Enterprises should care about U.S. E-911 Evolution*. 2002. COM-14-9382, Gartner Inc. January 22, pg. 1.
[52] "How Location Tracking will work", *Howstuffworks.com*, Retrieved: December 20, 2004, from http://people.howstuffworks.com/location-tracking.htm/printable, pg. 4.

In Canada, E-911 is still in its early days of network construction because, unlike the case in the U.S., where Phase 2 of their deployment is currently underway, [53] a nation-wide network has not yet been mandated by the federal government. A representative from a Canadian wireless vendor explains:

> In Canada the 911 service is a provincial law enforcement responsibility, but licenses have yet to be issued by the CRTC to deploy E-911 service, this is only being done for wire-line services [on a national basis]. At present, wireless service providers would be required to provide E-911 nationally but only where it was available provincially…so it's not a total mandate.[54]

Availability is, therefore, driven by the provincial governments and provincial carriers who are currently working at implementing this initiative. And they are still in the initial stages of providing the service.

Without pressure to develop nation-wide networks, it is easy to see how a patchwork of E-911 may offer service based on a caller's location in one area and not in another.[55] Industry representatives have noted that Rogers is still in Phase 1 of deploying its E-911 service, as are Telus and a number of companies that provide both the E-911 solution and the lawful intercept solution. This suggests that in Canada LBS for emergency response service can only provide the location of the closest cell-site to the caller, which could be quite far away. As mentioned in chapter 2, location technology continues to remain most commonly land-based or terrestrial in operation, using Assisted-GPS. This demonstrates a slow move towards taking advantage of the U.S. military's more accurate GPSS.

As one of the most widely used LBS applications, E-911 has also inspired organisations involved in security and public safety to deploy LBS for other purposes. Correctional facilities in the U.S. have made the switch from rudimentary electronic monitoring to LBS monitoring in their offender and parolee tracking programs. Upon release offenders's or parolees's whereabouts can be monitored and the surrounding community can be notified of their movements.[56] In some cities, police and emergency vehicle fleets have also been outfitted with Automatic Vehicle Location (AVL) technologies.

Another market driver for LBS is known as lawful access, defined by a Canadian wireless

---

[53] Phase 0: wireless calls are to be sent to a Public Safety Access Point (proprietary cell sites known in short as PSAPs). Phase 1: phone numbers must be displayed with all 911 calls, allowing the PSAP operator to call back if there is a disconnection. Phase 2: currently underway in the United States, this phase requires carriers to place GPS receivers in phones in order to deliver more specific latitude and longitude location information using an Automatic Location Identification (ALI), allowing for the identification of both phone number and location of the caller. One remaining obstacle is the upgrading of PSAP equipment to handle the newly embedded tracking technology. "When the upgrade is complete callers will be pinpointed to within 300 feet (91 metres) of their location." Ibid, pg. 4

[54] Interview, February 2, 2005.

[55] Some Canadian carriers have begun deploying initial upgrades for an E-911, LBS-enabled service for users, but this could also mean that if LBS are not built into the handset or greater steps are not taken to outfit cell sites with technology that can ensure greater accuracy users may not end up receiving effective, reliable service.

[56] "Law-enforcement agencies are learning the value of using GPS to keep a constant eye on some released prisoners", 2004. *The Feature*, July 12, Retrieved: February 12, 2005, from http://www.thefeature.com/article?articleid=100867.

industry association representative as an initiative that ensures law enforcement warrants are complied with by allowing access to conversations or wireless data through wiretapping. This may now include law enforcement acquisition of a user's location information.[57] In the U.S., lawful access or wiretapping laws are laid out in the Communications Assistance to Law Enforcement Agencies (CALEA), which mandates access to all wireless data that is non-proprietary from carriers and service providers during or leading up to an investigation. Prior to the events of September 11, 2001, there was much concern about the privacy implications of lawful access to any and all of a user's wireless communications, but post-9/11 such concerns have largely fallen on deaf ears.[58]

In Canada, the government is in the process of drawing up draft legislation that includes a thirty-month consultation process and some twenty closed meetings with industry, stakeholders and justice officials to address concerns and details of law enforcement requirements. Similar to lawful access requirements in the U.S., Canada is expected to incorporate a mandate that carriers and service providers will be required to supply access to law enforcement to monitor location and continued tracking of individuals, if they are to provide LBS. One representative of a Canadian wireless vendor explains that "given our understanding at this point, any new network equipment that is required to comply with such a mandate will have to be subsumed by carriers and service providers."[59] Regardless of the possible costs that will have to be incurred, compliance with lawful access will be total and may even push those involved in providing LBS to improve and increase their provision of such services. If carriers and service providers are already invested in LBS, they will most certainly be looking for ways to reduce the cost of compliance and may potentially ramp up the suite of LBS offered on the Canadian market.

Another market driver is the deployment of commercial-based applications of LBS in various business sectors. Commercial LBS have not moved carriers and service providers to upgrade their networks and handsets in the same way that the public sector initiatives have. However, those that have been providing particular sectors with LBS have managed to channel the one major benefit mobile phone service offers, "the fact that they directly address individuals."[60] LBS applications can be both carrier-based and sector specific-based such as in the cargo tracking sector. At present, Canadian carriers appear to be in favour of handset-based LBS systems. This would off-set some of the costs of running such a service, since customers would be required to purchase the LBS handset. Going with a network-based LBS system would require the carrier to pick

[57] Interview, February 2, 2005.
[58] Lyon, David. (2003). *Surveillance after September 11*. Polity: Cambridge.
[59] Interview, February 2, 2005.
[60] Blackwell, Gerry. 2001. "Location, location, location." *Wireless Telecom,* Vol. 19, No. 3, pg. 45.

up the majority of the upgrade costs. The handset model requires that new chips and antennas be integrated into handsets in order to offer individualized services such as navigational services or object tracking as discussed in chapter 2.

The opportunities to develop new revenue options and pitch services directly to individual needs are endless and could become increasingly attractive as LBS is integrated with a "rise in complementary technologies such as digital mapping and wireless communication peripherals."[61]

However, at this time the Canadian market players remark that there is currently no carrier that is actively pursuing/promoting LBS simply because they have not deployed the networks in their entirety. Currently, Telus and Bell Mobility are the only companies to conduct field trials of assisted-GPS LBS in their handsets. "In 2001, Telus gave 100 customers in Toronto access to a range of web-based services including an E-411 service that let them call an operator and get directions to the nearest restaurant, gas station or bank machine."[62] Bell Mobility has also conducted a trial, albeit even smaller, involving 50 customers to test customer perceptions of privacy and design and to evaluate the demand for different types of applications through their integrated handset-based receiver.[63] In discussion with other Canadian industry representatives Bell Mobility is also set to introduce an assisted-GPS LBS enabled handset to market in 2006.

Apart from carrier involvement in LBS, there have been various applications provided by Canadian companies such as Cell-Loc and Cellocate for use in truck and taxi fleet tracking systems, using either satellite-based GPS or Time Difference of Arrival (TDOA) technology. Such companies act as providers of middleware and are largely independent of the carriers (particularly in running their own location technologies) apart from overlaying their services onto a carrier's network. For example, Rogers has been offering such access to service providers since the late 1990s.[64] Some service providers have stated that they feel like they are forever waiting for a carrier to break into the commercial LBS market. At this time, industry representatives in Canada are unaware of "anywhere in the world where there is actually a viable position location service."[65]

Canadian Market Realities

With so few commercial applications being marketed in Canada, it is difficult to clearly identify present patterns of use, future participants in the market, or any substantial trends concerning future LBS deployments. Many industry experts are now forecasting a protracted introduction of LBS. Other Canadian LBS companies such as Boomerang, Profillium, AirIQ and Ewireless Canada Inc.

[61] Tristram, Claire. 1999. "Has GPS lost its way?" *Technology Review*, Retrieved: February 7, 2005, from http://www.technologyreview.com/articles/99/07/tristram0799.asp?p=1, pg. 73.
[62] Blackwell, Gerry. 2001. "Location, location, location." *Wireless Telecom,* Vol. 19, No. 3, pg. 43.
[63] Ibid, pg. 43.
[64] Interview, March 1, 2005.
[65] Interview, March 1, 2005.

appear to be leading the industry; however, larger potential LBS providers remain hesitant to make a substantial investment. As one Canadian wireless industry consultant points out, "They [carriers] don't want to be the first guy on the block with location services and have articles in newspapers saying location services are great, but now here are all these concerns."[66] Therefore the arrival of LBS in the Canadian market is very sluggish and little is known about usage rates, size of investments and possible key clients.[67] "Most Canadian service providers (including carriers) are following the lead of the U.S.; that's what will drive the technology."[68] Canada has, therefore, taken a wait-and-see approach to observe how LBS is unveiled in the U.S.[69] Hence, despite enthusiastic market forecasts a number of years ago, results have not fallen in line with the predictions, particularly in Canada. However, both current service providers and carriers are expressing some optimism. As one industry analyst put it, "they are playing it [their strategies] somewhat close to the vest. And that is a sure sign they believe there's serious money in it."[70]

Market Impediments

Given that the Canadian LBS market is said to be banking its future on increased deployment of LBS in the U.S. market, an assessment of any challenges or impediments to LBS development are summarized in this section. In both public and private sector deployments, impediments appear to be based mainly on operational/design challenges as well as compliance and standardization hurdles.

One of the most significant impediments to LBS development is in the cost of deploying location technologies. Smaller companies may have an easier time with providing solutions from scratch and the ability to form an overlay structure that is then connected to a main carrier's network. However, wireless carriers, which have incredibly large and complex networks, will have to go to considerable lengths and expense to provide the appropriate upgrades and integrate new technology requirements for both handset- and network-based design within the existing infrastructure. As stated by a Canadian wireless vendor, "the complexity of a carrier's network can be mind-boggling…If you were to see an actual schematic or network diagram of Rogers' network across the country, it would fill a fairly large wall."[71] There are also considerable concerns that technology costs have contributed to a current "lack of standard interfaces and no broad-based enterprise or consumer-oriented applications."[72]

For LBS offered by carriers to be viable, "operators must be able to offer a broad portfolio of services with compelling applications and content that is attractively priced."[73] However such a feat would be

[66] Interview #2, March 1, 2005.
[67] Interview #1, March 1, 2005.
[68] Blackwell, Gerry. 2001. "Location, location, location." *Wireless Telecom,* Vol. 19, No. 3, pg. 40.
[69] Ibid, pg. 43.
[70] Ibid, pg. 46.
[71] Interview, February 23, 2005.
[72] *Enterprises should care about U.S. E-911 Evolution*. 2002. COM-14-9382, Gartner Inc. January 22, pg. 1.
[73] *Mobile Location Services: No Mass Market in Europe Until 2007*, 2001. Gartner Inc., July 9, pg. 1.

difficult to accomplish if both the technology itself and the integration of it remain inappropriately priced. There are reasons for potential operators to be optimistic; however, when some location technologies such as GPS-enabled chips are observed from a cost perspective. "[GPS-enabled chips] are sinking in price…which are following Moore's Law with a vengeance and will soon be available for about $10 [USD]…with basic hardware that's cheap, it becomes economical to embed GPS in cellphones, pagers and dashboards, without significantly raising the price of these items"[74] or the services provided.

The way in which carriers deploy pricing strategies can also drive down the popularity of LBS with customers. A 2002 Gartner survey, found that there was a significant correlation between the provision of LBS, frequency of use and price per use of service. Over the last few years service providers and carriers have generally only offered highly priced query rates.[75] In the case of tracking vehicles, where vehicles are tracked in real-time, a location query would have to occur every few minutes. Highly priced usage rates can therefore limit market access to those who view such tracking as a business necessity rather than just an advantage. It, therefore, impedes popularity and widespread use of real-time tracking.[76]

In addition to the high-priced license fees that carriers and service providers already pay, the challenge of maintaining a desired profit margin increases when carriers must comply with government initiatives such as E-911 and lawful access. As mentioned, E-911 and lawful access, particularly in the U.S., have required that carriers subsume the cost of upgrading their networks and equipment to ensure compliance with emergency response and law enforcement requirements. Carriers may also face additional costs if compliance is not instituted within mandated time frames. In 2002, AT&T failed to launch location-enabled handsets by the Phase 2 deadline of the E-911 initiative and in turn, was fined $2.2 million USD by the FCC.[77]

There is also a significant correlation between accessible, efficient and accurate location technology design and the widespread use of LBS. Currently there are several operational and technological impediments keeping LBS from drawing a larger customer base. The very nature of E-911's efficient service prospects relies on ubiquitous positioning of cell sites as well as upgrades to equipment and **public safety answering points (PSAPs)**. Ensuring this is a monumental task that has required years of preparation and which has had varied results in service within the U.S. As one Canadian carrier representative points out, U.S. tests have even shown PSAPs to be ineffective at receiving individual location data because the

[74] Tristram, Claire. 1999. "Has GPS lost its way?" *Technology Review*, Retrieved: February 7, 2005, from http://www.technologyreview.com/articles/99/07/tristram0799.asp?p=1, pg. 73.
[75] When converted from euro cents into Canadian cents, query rates per usage can range from 34-75 cents. Respondents of a Gartner survey, polled in 2002, stated that in order for the service to be both cost-effective and widespread in its use, query rates per usage should range from 15-8 cents. *European Symposium Mobile Technology Survey.* 2002. COM-14-9382, Gartner, Inc. January 22, pg. 3.
[76] Ibid, pg. 3.
[77] *Enterprises should care about U.S. E-911 Evolution*. 2002. COM-14-9382, Gartner Inc. January 22, pg. 1

public safety system has yet to appropriately upgrade their own infrastructure to meet the technological requirements that the carriers have set up. This has resulted in access to E-911 in some areas and not in others because "the technology and setup is insufficiently dependable to justify any form of mandate."[78]

There is also concern that embedding GPS technology into handsets will cause other functions in the mobile phone to become inefficient or ineffective. "GPS technology could even hog a phone's processing power to the point that it could not triangulate a location and support a voice call at the same time."[79] A customer could request information based on their real-time location and end up with a handset that is drained of its power in a very short amount of time. Similar concerns apply to network-based solutions, where "the computing power required to constantly track millions of users would be enormous and the use of network bandwidth highly inefficient."[80] In addition, carriers have to worry about the problem of trying to enable all of the handsets that have previously been sold so that more customers could sign on to LBS. Waiting for customers to turn in their old mobile phones for new GPS enabled handsets could take up a formidable amount of time. Incentive strategies might hurry the process but with further expense to the carrier, not to mention exacerbated waste concerns.

The appropriate provision of accuracy of location can also be a problem. "Network-based solutions may not be accurate enough to enable some applications, such as automatically dispatching a taxi cab based on very precise location information."[81] As mentioned in chapter 2, most location technologies can lose much of their accuracy if a user is no longer in line-of-site with at least three cell sites or satellites. "A 120 metre error range may let you spot a flashing restaurant sign down a city block, but even a five-metre miss in a skyscraper could put a user on a completely different floor."[82] Again, cost becomes a factor because carriers must deploy complementary Wi-Fi networking technology for indoor use of LBS to avoid such problems.

Like most other deployments of technologies, impediments also include incompatible services, technologies and poorly designed applications. Given the ongoing improvement of location technologies and services many forecast that such impediments will shortly become a thing of the past. However, larger considerations arising in relation to information privacy, data security and related social issues may plague LBS investors for a much longer time if not appropriately addressed at the policy level in Canada and elsewhere. Chapter 4 addresses such issues in conjunction with public attitudes and industry marketing strategies.

[78] Interview, March 1, 2005.
[79] Blackwell, Gerry. 2001. "Location, location, location." *Wireless Telecom,* Vol. 19, No. 3, pg. 45.
[80] Ibid, pg. 45.
[81] Ibid, pg. 45.
[82] Ibid, pg. 45.

Chapter 4
Information Privacy and Data Security: Corporate Strategies and Public Attitudes

Introduction

Attitudes towards the potential use or misuse of location data and personal information are likely to be influenced by relevant government policies, commercial initiatives, and by representations in the popular media

In this chapter, we identify the most pressing concerns surrounding the deployment and use of location technologies and services in relation to information privacy and data security in Canada. As indicated in the introduction to this report, our primary focus is on LBS use. The chapter is divided into two main parts. Part I draws attention to questions of personal and location information use as they pertain to the marketing strategies of relevant wireless carriers and service providers. While the main emphasis is on commerce, attention is also given to privacy issues likely to arise in the workplace, as well as in the areas of law enforcement, emergency response and other contexts involving the state's relationship to its citizens. In addition, examples are provided to illustrate the ways in which privacy issues arising in both the public and private spheres may converge. Part II considers data security in terms of the types of guarantees that carriers and service providers may offer their customers with respect to their personal and location data. Related issues concerning public attitudes are addressed in both sections.

Our research findings suggest that major wireless carriers and location-based service providers in Canada will likely be proactive in anticipating and addressing public/legal concerns with respect to the appropriate collection, use and disclosure of customer information. Conversely, there may be more reluctance on the part of many businesses to invest the resources needed to head off potential problems in the area of data security. Significantly, the greatest threats to the security of customer information collected by location-based service providers are unlikely to be directly related to their use of location technologies *per se*. While problems involving the unlawful acquisition of real-time location data may arise in some instances, such occurrences will likely be rare and will almost certainly be dwarfed by situations in which customer information warehoused in computer databases has become compromised. In this respect, the information privacy concerns facing subscribers to LBS are not unique, and continue to confront the users of countless commercial products and services. What is unique, however, is that the information gathered and stored in these databases will enable a more comprehensive picture of individual and collective patterns of movement. This, in turn, will invite the creation of new algorithms designed to make inferences concerning the potential relationships between mobility and identity.

Evidence suggests that public attitudes concerning information privacy are highly malleable. In addition to being conditioned by a variety of socio-economic and cultural variables, attitudes towards the potential use or misuse of location data and personal information are likely to be influenced by relevant government policies, commercial initiatives, and by representations in the popular media.[83] In fact, an understanding of consumer attitudes as amenable to cultivation already informs the marketing strategies of industries hoping to benefit from the widespread introduction of LBS. It is primarily for this reason that public attitudes are being addressed here in conjunction with relevant corporate and governmental practices. In addition, the often complex interrelationships between public opinion, commercial activity and government policies draw attention to some of the limitations, which are arguably inherent in more traditional approaches to questions of privacy, particularly those which focus exclusively on the rights of

the individual citizen or consumer. Some of these limitations are briefly commented upon in this chapter before receiving closer attention in chapter 5.

Part I: Information Privacy

As indicated in chapter 3, location-based services (LBS) have yet to become well established in Canada. However, carriers and service providers continue to believe that services which enable them to locate subscribers will become very important in the near future.[84] The future growth of LBS clearly has privacy implications for consumers. The use of location-based technology in conjunction with wireless technology adds geographical location data to the catalogue of personal information that is already routinely collected from users. In fact, relevant privacy issues have already surfaced as a result of business practices in the relatively new area known as mobile commerce (m-commerce).

As Gratton has indicated, privacy issues arising in relation to m-commerce, and which involve the use of locational information, can usefully be separated into two categories. [85] The first concerns customer tracking over time. Increasingly sophisticated profiles of a customer's travel patterns, movements and other habits may be constructed through the use of historical location data stored in databases. The second area concerns the commercial use of real-time location data. Data of this type may be used to send location-specific advertisements to the wireless user.

According to Green and Smith, "location data involves the categorical association between devices, the information generated through them, and the people to which they are attached."[86] However, it is important to emphasize that the location data potentially generated by subscribers to location-based services (LBS) using GPS enabled technologies such as cellphones or PDAs are not synonymous with personal information *per se*.[87] Gratton suggests that location data may be considered personal information "if and only if it contains personally identifiable information which has been defined as data that can be used to contact a person uniquely and reliably, including but not limited to name, address, telephone number, and email address."[88]

The success of m-commerce hinges upon the effective use of location-based advertising. Significantly, location-based advertising provides businesses with the potential opportunity to bridge the prediction of wireless users preferences and buying patterns with direct marketing targeted to the exact moment and location of the consumer.[89] By making use of real-time location data, marketers may deliver advertisements to the wireless user at a

[84] *Wireless Services for Telematics Have Yet to Thrive*. 2002. Technology Analysis, Gartner Inc., July 23, pg. 1
[85] Gratton, Eloise. 2002. "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising". *Canadian Journal of Law and Technology*. Vol. 1, No.2, November, pg. 71
[86] Green & Smith. 2004. "A Spy in your Pocket? The Regulation of Mobile Data in the UK." *Surveillance & Society*. 1 (4). (573-587)
[87] Gow, Gordon. *Pinpointing Consent: Location Privacy and Mobile Phones*. paper prepared for 'The Global and the Local in Mobile Communication' conference. June 10-11, 2004. pg. 10
[88] Gratton, Eloise. 2002. "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising". *Canadian Journal of Law and Technology*. Vol. 1, No.2, November, pg. 61
[89] Ibid. pg. 73

time and place which would make the message particularly relevant. An example would be a text message received via cellphone by a user passing by a particular business establishment. The advertisement in question might concern a sale underway at that location. Clearly, such instances may be experienced as highly intrusive if unanticipated by the user.

While Canadian carriers and service providers undoubtedly hold an interest in promoting m-commerce, evidence suggests that most of them will be cautious with respect to the collection and release of customer information. As one representative of a leading Canadian wireless industry association emphasized, Canadian cellphone users now approximate the 15 million mark, and maintaining good relationships with customers largely depends upon the ability to offer guarantees in the areas of customer information use and data security.[90] This source also indicated that wireless carriers will be wary of application developers claiming that they "have the number one product and we want to give it to your customers." Any such claims would have to be assessed very carefully to make sure that they do not interfere with the privacy concerns of real or potential customers.[91] However, there is a strong possibility that issues of data security may not be as readily addressed by industry as are matters surrounding the correct collection and use of personal information. This point is re-visited in the second section of this chapter.

On the whole, industry appears eager both to allay potential customer anxieties about privacy and to cultivate positive public attitudes towards practices of m-commerce and the provision of LBS more generally. Furthermore, it seems likely that most major wireless carriers and service providers will be motivated to provide opt-in information policies even in the absence of legal coercion. The business logic of doing so is underscored in statements made by Gartner Research, which has advised its clients that:

> Services that use location data have great potential for improving customer relationship management. Unfortunately, they also have great potential for annoying existing and potential clients. We believe that the most successful implementations will use "opt-in" rather than today's internet model of client "opt-out."[92]

According to one member of a Canadian wireless industry association, there are no working groups presently considering the use of "push" applications to send unsolicited email to potential customers. Instead, this interviewee referred to the growing importance of a form of text messaging referred to as "common short codes."[93] The use of these codes is available to all wireless carriers and has been in use for about two years. During an interview, our source described the usefulness of common short codes as follows:

[90] Interview: March 2005
[91] Ibid.
[92] *User Location Will Help Business*. 2005. AV-13-7291, Gartner Inc., pg. 3.
[93] Interview: March 2005

> …to start a relationship with a wireless phone user, whether you wanted to involve them in a trivia contest or whether you wanted to offer them a coupon for your café… you can advertise in some other source, whether it's a billboard or whether it's on your product itself or whether it's in newspaper advertising or on line, on the radio saying that if you have a wireless phone and you would like to receive a coupon from Betty's café, send the word coffee to Betty and that would actually translate into an actual digital number like 56784. …By doing that, you're asking them to send you something.[94]

While leading carriers and service providers in Canada will likely wish to avoid alienating customers with unsolicited SMS, the same may not hold true with smaller businesses or those operating outside the country. Text-messaging problems resulting from the use and sale of location data have already been experienced in the U.K. where increasing numbers of mobile business operators have made data available to application and content providers on a wholesale basis. Location brokers are also emerging with connections to the location feed of multiple carriers, who then resell this data to third parties.[95] Text-messaging problems have also arisen south of the Canadian border. A recent study conducted in the United States by the Pew Internet and American Life Project found that 28 percent of people who utilize text messaging on their cellphones have received unsolicited commercial messages in that form.[96]

According to Green and Smith,[97] as practices of m-commerce continue to mature in the U.K., leading mobile business operators are becoming increasingly outspoken in their insistence that SMS spamming practices hurt m-commerce as a whole. However, despite this recognition on the part of better established commercial interests, spamming remains irresistible to many smaller businesses due to the low barriers to becoming an m-operator and the high profitability that spam offers. SMS advertising practices in the U.K. have typically had response rates of 20 to 30 percent.[98] Consequently, this particular form of privacy invasion appears likely to remain a nuisance for the foreseeable future.

Regulation guidelines in the specific areas of LBS and text-messaging are generally less clear in North America than in Europe.[99] For example, Gratton[100] argues that legislation is often vague with respect to the requirement that location service providers disclose the purpose of obtaining location data, and cites the following considerations as requiring closer attention: Who should be provided with disclosure?, Who be responsible for providing disclosure?, How should the disclosure be given?, When should disclosure be given? and What should be the content of disclosure?

---

[94] Interview: March 2005
[95] "Privacy: Commercial MLS launches are delayed by fears of 'Big Brother'". *Mobile Location Analyst*. Oct. 2003. pg. 5
[96] "Study: 'Texting on the Rise'", 2005. *Associated Press*, March 17.
[97] Green, Nicola and Smith, Sean. 2004. *Regulation, Information and the Self: Ownership in Mobile Environments*. pp. 39-40.
[98] Ibid. pg. 40.
[99] "Privacy: Commercial MLS launches are delayed by fears of 'Big Brother'". *Mobile Location Analyst*. Oct. 2003. pp. 7.
[100] Gratton, Eloise. 2002. "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising". *Canadian Journal of Law and Technology*. Vol. 1, No. 2 November, pg. 63.

Gratton also points to legal grey areas in terms of customer consent and lists the following as needing further clarification: From whom do you get consent?, Who should be responsible for consent? and How should consent be obtained?[101]

The questions raised above are important and draw attention to some of the unique policy challenges arising from the commercial use of location technologies. For example, the information needed for sufficient disclosure of commercial privacy policies, or to obtain consumer consent for a service would be difficult to render via the small screens built into wireless devices. Presently, such screens may only hold up to 160 characters. While alternatives in the form of signed agreements may be found, related difficulties may still arise. For example, debates still continue over whether disclosure should take place before data is collected, or before it is used.[102] This issue is complicated by the fact that commercial uses for locational or personal data may change over time. How often consent should be requested by service providers remains an unresolved issue.

It should be kept in mind that in wireless communication networks, data which give the geographic location of users, or more accurately their location equipment, already exists. This information is necessary to enable the transmission of communications to and from users without fixed locations, a fact which makes the entire issue of disclosure problematic. At the same time, the ability of networks to locate devices rather than specific individuals may call into question the value of location data for some emergency purposes. It is interesting to note that in Canada, it has primarily been public safety agencies which have been pushing for real-time disclosure of wireless subscriber list information. Conversely, wireless carriers have taken the position that such information would be meaningless when calls are placed from cellphones having no fixed association with a subscriber's home or business, or even with a particular individual.[103]

The question of who owns a person's locational data remains a highly contentious issue. Mobile network operators may assume that they own such data since they are gathered from their networks. Conversely, many privacy rights advocates argue that subscribers are the rightful owners of their location data.[104] As indicated above, however, the location of a device may or may not correspond to that of a specific user. The question of ownership becomes even murkier once location data is sold on by carriers to third-party application and content providers, or mobile marketing firms. The question then arises as to whether the ownership of data gets transferred from party to party as it moves down the value chain.[105]

---

[101] Gratton, Eloise. 2002. "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising". *Canadian Journal of Law and Technology*. Vol. 1, No. 2 November, pp. 63-66.
[102] Ibid. pg. 63.
[103] Gow, Gordon A. 2004. *Prepaid Mobile Phone Service: the Anonymity Question*. pg. 7.
[104] "Privacy: Commercial MLS launches are delayed by fears of 'Big Brother'". *Mobile Location Analyst*. Oct. 2003. pg.19

As previously indicated, the success of m-commerce and accompanying practices of location-based advertising are premised upon the idea of personalized service, whereby customer information is ostensibly used by business to better respond to a customer's stated or perceived needs. Citing recommendations made by Forrester Research, Gratton[106] observes that the best content providers deliver context-relevant advertising, and that this in turn makes wireless users more accepting of location-based services and advertising on the whole. The clear implication is that commerce hopes to encourage a longer term trend in which customers feel increasingly comfortable volunteering personal or location data to marketers. Hence, the objections which well established commercial interests have made to practices such as SMS spamming, are also indicative of their eagerness to shape public attitudes in ways that will benefit m-commerce over the long-term.

Even perfectly legal marketing practices which ostensibly respect the rights and autonomy of consumers are worth considering in relation to issues of privacy and surveillance. They draw attention to the unequal power relationships between industry and consumers, and may help explain the inconsistency of public attitudes to privacy. The same holds true with respect to relevant initiatives on the part of governments. For example, it is worth noting that the m-commerce business strategy referred to above has found parallels in similar efforts to introduce surveillance and tracking technologies to the public on the part of both industry and governments in various parts of the world. In each case, a phased approach has been adopted that is designed to assuage public concerns about privacy while encouraging new habits on the part of targeted populations.

A report by Gartner Research argues that while the adoption of ID cards for financial functions is often a slow process, if done correctly, it can prove extremely successful.[107] The report cites the examples of the "Octopus card" in Hong Kong, and the Cashcard system now used in Singapore for road tolls. Both cases were used to demonstrate that "the successful development of a smart card culture first requires adoption in a ubiquitous function that, once changed, will improve the user's life."[108] In the case of Hong Kong, the report notes that about eight years ago the public was provided access to a card that shortened waiting lines at train stations and bus terminals. Later, people came to recognize that the card could improve their shopping or transportation experience. Consequently, fast-food outlets, convenience stores and other enterprises began to use this technology. Eventually the population became accustomed to using smart cards for daily transactions.[109]

[105] "Privacy: Commercial MLS launches are delayed by fears of 'Big Brother'". *Mobile Location Analyst*. Oct. 2003. pg.19.
[106] Ibid. pg.60.
[107] Gilliland, Martin. 2003. "Smart Cards, Smart IDs and the Semiconductor Industry". Gartner: Research Brief. July 28, pg. 3.
[108] Ibid. pg. 5.
[109] Ibid. pp. 3-4.

In the case of the Cashcard in Singapore, the same report notes that the card's use for public transportation also meant its adoption by the overwhelming majority of the population in most urban centres. The significant investment in infrastructure will allegedly have future pay-offs; "the next step may be for the cards to be used for more secure financial transactions, such as credit cards."[110] Taking this logic further the report asserts that "once people become comfortable enough with smart card technology to use it for their credit card and banking transactions, government should encounter far less resistance from the public when choosing this technology for identification purposes."[111] While the report acknowledges that strong initial resistance to smart cards may be encountered in some instances, it also suggests that the development of necessary infrastructures and the gradual extension of card functions to new services will eventually help overcome it.

The examples cited above are worth holding in mind when considering the development of LBS in the United States. In line with recent E-911 legislation, the Federal Communications Commission (FCC) now demands that records of customer location patterns be kept for public safety reasons. This legislation was passed due to the growing number of cellphone users in combination with the fact that the location of a mobile telephone could not be assumed to reside at a particular postal address.[112] However, with LBS imperatives, industry standards in the U.S. now also include the storage of locational data for future marketing use. Significantly, such data may readily be used not only to target advertisements to consumers, but also to gather information concerning the "mobility of populations" which is then used to create "idealized places, products, markets, and consumers."[113] What is noteworthy here is that commercial practices which involve the sophisticated use of anonymous, aggregate data to categorize consumers into specific target groups, have flown beneath the radar of existing privacy laws in the U.S.[114]

In the U.S. and Canada, privacy laws are ostensibly designed to protect the individual from unsolicited harassment and to safeguard the use of personal information. This orientation is readily visible in those sections of the PIPEDA which address the commercial use of customer information. Section 5.3 of the Act specifies that an organisation "may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate under the circumstances."[115] However, while such legislation is clearly necessary to protect the rights of individuals, it is not designed to deal with the commercial social sorting practices made possible through the use of anonymous aggregate data.[116]

---

[110] Gilliland, Martin. 2003. "Smart Cards, Smart IDs and the Semiconductor Industry". Gartner: Research Brief. July 28, pg. 5.
[111] Ibid.
[112] Curry, Michael R, Phillips, David J. and Regan, Priscilla M. 2004. "Emergency Response Systems and the Creeping Legibility of People and Places". *The Information Society*, Vol. 20, pg. 366.
[113] Ibid. pg. 367.
[114] Ibid.
[115] Privacy Commissioner of Canada, 2000. *The Personal Information Protection and Electronic Documents Act*, Available: http://www.privcom.gc.ca/legislation/02_06_01_e.asp.
[116] "Privacy: Commercial MLS launches are delayed by fears of 'Big Brother'". 2004. *Mobile Location Analyst*. October. pg. 8.

Similarly, Canada's Privacy Act (1982), which regulates the use of personal information by the state, was not designed with the privacy implications of location technologies in mind. This point is noteworthy since it is the state which arguably has the largest interest in tracking population movement. Tracking technologies may prove exceedingly valuable not only for purposes of law enforcement, but also for planning in the areas of social policy and infrastructure. The 407 Express Toll Route (ETR), which runs north of Toronto, is a case in point. While not a location technology in the strict sense defined in this report, its construction highlights the degree to which a new generation of closely interrelated technologies have come to provide governments with powerful tools for rendering the movements and habits of populations more visible.

The 407 ETR runs north of the far more congested highway 401. Begun in 1993, its extensions now stretch 108 kilometres through one of Canada's most densely populated urban environments and busiest transportation corridors.[117] With more frequent interchanges than any similar highway, the 407 ETR is currently the only multiple entry and exit automatic toll road in existence. In terms of addressing individual privacy concerns this highway arguably represents a great success. It has been heralded by the Ontario Transportation Capital Commission as the first Intelligent Transportation System in the world to allow users to travel anonymously. The system has several built-in safeguards to protect driver identity: cameras designed to photograph only the rear license plates of cars (not fronts, interiors, etc.); the use of acquired personal information only for toll collection, traffic management and its own marketing purposes; and tight contractual clauses between the Ministry of Transportation and 407 International Inc. ensure that the **confidentiality** of personal information is protected.[118]

Despite such safeguards, the existence of highway systems such as the 407 ETR, raise important ethical social concerns. For example, there is always the possibility that segregated forms of transportation will become entrenched. Significantly, those who can afford it now subject themselves to a different kind of surveillance, one based on checkpoints and transponders rather than traditional forms of policing. Furthermore, it appears likely that systems such as the 407 ETR will eventually be overtaken by cellular and geographic information system (GIS) technologies. Roughly 28 percent of Canadian vehicles now contain cellular devices.[119] Researchers Bennett, Collins and Raab[120] have observed that "the smart vehicle of the future will record location information, and cellular operators will collect it for governmental use." They note further that:

[117] Bennet, Colin; Raab, Charles; Regan Priscilla. 2003. Patterns of individual identification within intelligent transportation systems. In *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. (153-175), pg. 157.
[118] Ibid. pg. 159.
[119] Ibid. pg. 160.
[120] Ibid. pg. 161.

> The efficiencies of on-board cellular and GIS tracking technologies for a range of public and private purposes will likely present far greater challenges to individual privacy than the relatively discrete and manageable highway system on Toronto's route 407.[121]

Not surprisingly, the ability to track the location of vehicles has already raised new concerns with respect to employer/employee relations. Just as marketers wish to gather information on real or potential customers and governments want to monitor the identities and movements of citizens, employers are always on the lookout for new ways to keep tabs on their workers. Clearly, the use of location technologies such as those enabled by GPS technology greatly enhance the ability of management to watch over and control the activities of mobile workers. This may in turn lead to more productive and, in many cases, safer work environments. At the same time, greater scrutiny of worker behaviour may mean increased levels of stress for employees while providing a potential basis for new forms of discrimination in the workplace.

While location technologies may readily be used to extend centralized control, their introduction to the workplace may also have a destabilizing or transformative effect upon established routines and procedures. For example, the management of a news channel in Washington D.C. now monitors the locations and movements of reporters and photographers through the use of GPS. Union concerns were raised after at least two workers were disciplined for inappropriate use of vehicles. One news photographer indicated that since the installation of GPS in vehicles, workers have become less certain of the rules pertaining to vehicle use. This individual stated that "we all understand we can't take the company car to go to Ocean City for the weekend. But is it okay to pick up milk or pizza on the way home? All of these were never questioned before we go to the GPS system."[122]

GPS technology has increasingly been used for purposes of fleet management, a fact which has clear consequences for drivers. For example, GPS is now used by many companies to keep track of the activities, movements and locations of truckers. This includes vehicle data such as maximum speed, vehicle location, gas consumption and the length of time stopped at various locations.[123] Such information may readily be used for comparison with what the drivers fill out in their logbooks and timesheets.[124] These points are significant, not only because they may engender distrust between management and drivers, but also because the judgements made by employers based on such data may be flawed. For example, a trucker may use his or her discretion to avoid a traffic jam or construction, while in

[121] Bennet, Colin; Raab, Charles; Regan Priscilla. 2003. Patterns of individual identification within intelligent transportation systems. In *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. (153-175), pg. 161.
[122] Baker, Chris. (2003, January 23). "Channel 7 uses GPS to dispatch its crews: Some workers see privacy violation." *The Washington Times*. pg. C11. Available www.global.factiva.com
[123] Kumar, Sameer & Kevin Moore. 2002. "The Evolution of Global Positioning System Technology." Journal of Science and Education Technology. 11 (1). pp. 59-80.
[124] Murphy, Shannon. (2004, July 1). "How to Choose a GPS Fleet Management System: What Features are Right for You?" Management Quarterly. 45 (2). pg. 30. Available www.global.factiva.com

the eyes of management they are simply deviating from planned routes. Alternatively, if a driver stops at a medical clinic and this is conveyed to the employer, erroneous conclusions may be drawn. As Introna has made clear, there is always a strong possibility that inaccurate inferences will be drawn from location and movement information.[125]

More fundamentally, the use of location technologies and other surveillance technologies in the workplace usually implies that management either does not trust the motives of its employees, questions their competence or both.[126] This fact has certainly not been lost on workers and their unions, and it has led to resistance to the use of location technologies in many cases. For example, after radar location devices were installed in the vehicles of Boston police officers, some officers responded by smashing the devices with their nightsticks.[127] Unions have also objected to GPS tracking of employees or their vehicles. The Teamsters Union fought against the management of the United Parcel Service when the latter wanted to install GPS in workers' vehicles. Eventually the teamsters signed a new contract which barred the use of GPS for evaluation purposes.[128] In another instance, the union for city workers in Chicago challenged their employer who wanted workers to carry GPS-enabled cellphones at all times. In this case, a compromise was worked out in which the cellphones can be turned off during lunch and after work hours.[129]

Significant privacy issues concerning the acquisition, use or misuse of personal and location information may also arise in the areas of law enforcement and emergency response. Potential problems in these areas may involve direct threats to specific persons by someone known to them. For example, in the case of law enforcement it cannot simply be assumed that those authorized to track others will never be driven by unprofessional motives such as personal grudges or jealousy.[130] In addition, increasingly sophisticated forms of surveillance and information gathering such as those associated with emergency response initiatives may invite other forms of corruption and power abuse. As Phillips, Curry and Regan observe with respect to the E-911 initiative in the United States:

> A system that singles out individuals within a particular area and warns them of impending danger is very much like one that creates a list of all people who disagree with a particular political policy, or who have openly voiced concern about a particular leader.[131]

---

[125] Introna, Lucas D. 2003. "Workplace Surveillance 'is' Unethical and Unfair." *Surveillance & Society*. 1 (2). pg. 214.
[126] Zureik, Elia. 2003. Theorizing Surveillance: The Case of the Workplace. In, David Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*.
[127] Marx, Gary T. 2003. "A tack in the Shoe: Neutralizing and Resisting Surveillance". *Journal of Social Issues*. 59 (2). pp. 165-189.
[128] Baker, Chris. (2003, January 23). "Channel 7 uses GPS to dispatch its crews: Some workers see privacy violation." *The Washington Times*. pg. C11. Available www.global.factiva.com
[129] Charny, Ben. (2004, September 24). "Big Brother Likely to Be Big Boss." *The Atlanta Journal*. pg. A1. Available www.global.factiva.com
[130] "Privacy: Commercial MLS launches are delayed by fears of 'Big Brother'". 2003. *Mobile Location Analyst*. October. pg. 5.
[131] Curry, Michael R., Phillips, David J. and Regan, Priscilla M. "Emergency Response Systems and the Creeping Legibility of People and Places". *The Information Society*, 20: 2004. pg. 361.

As Marx emphasizes, surveillance techniques provide the powerful with new means to monitor and intimidate enemies.[132] Precedents certainly have been set in cases where individuals or groups have been targeted by powerful interests for personal or political reasons. For example, Marx notes that J. Edgar Hoover was notorious for intimidating political enemies through use of the extensive files he kept on important people. Marx also cites numerous cases in which mayors and police chiefs at the municipal level have used surveillance techniques to harass or intimidate people or groups, or attack their reputations.[133]

The practices of personal and location information gathering needed to ensure the effectiveness of E-911 have other direct privacy implications pertaining to law enforcement. Unlike the examples cited above, however, the main issue here concerns the *legal* procurement of personal information. Curry, Phillips and Regan note that the locational and personal information gathered for purposes of E-911 will likely be available to law enforcement under simple subpoena or court order.[134] It seems equally likely that the continued development of a similar system in Canada will provide law enforcement in this country with ever more precise and revealing data on individuals suspected of committing illegal acts. At the same time, such developments will likely go unnoticed by many or most citizens.

It is worth reiterating that most major carriers and service providers in Canada will likely be able to adapt themselves to the opt-in principle upheld in the PIPEDA. At the same time, the state practices, workplace issues, and marketing strategies discussed above underscore the relative vulnerability of citizens, consumers, workers and travellers. As Green and Smith[135] have observed, the primary relationship between organisations and individuals continues to remain one of "asymmetric surveillance"; this reality will receive closer attention in chapter 5.

Part II: Data Security

In addition to concerns about the collection, use and potential misuse of personal or location information, numerous concerns have arisen in relation to personal and location data security. As noted by wireless technology expert David Crowe,[136] wireless communications are particularly vulnerable to security problems because there is no way to protect the communications link. A recent report in *ComputerWeekly.com* notes that the ease with which wireless access points can be installed increases the risk of unauthorized access to wireless networks.[137] The report also notes that for companies looking to implement wireless technology on their networks, one of the greatest concerns is preventing the network from being visible to those outside and close to

[132] Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. University of California Press: Berkeley. pp. 138-141.
[133] Ibid.
[134] Curry, Michael R., Phillips, David J. and Regan, Priscilla M. "Emergency Response Systems and the Creeping Legibility of People and Places". *The Information Society*, 20: 2004. pg. 366.
[135] Green, Nicola and Smith, Sean. 2004. *Regulation, Information and the Self: Ownership in Mobile Environments*, pg. 80.
[136] Crowe, David. 2004. "Wi-Fi, Wi-MAX: Taking wireless security seriously". *Wireless Telecom,* Issue Three, pg. 36.
[137] Connolly, Allison. 2005. "Securing your networks against the risk of rogue wireless access is no longer optional". *ComputerWeekly.com,* January 25, Available: http://www.computerweekly.com.

the business premises. For example, individuals parked in cars close to a building may use personal wireless devices to tap into radio frequency leakage from the building to gain access to company information. While such leakage may be reduced, it is widely acknowledged that it is almost impossible to eliminate it entirely.[138]

Another data security problem involving surreptitious access to a network might arise when users of Wi-Fi laptops, cellphones or other wireless devices attempt to gain access to the internet through the use of hotspots. In some cases, the access points being tapped into may actually be "evil twins."[139] In such instances, users think they've logged on to a wireless hotspot connection when in fact they've been tricked into connecting to the attacker's unauthorized base station. The attacker jams the connection to the legitimate base station by sending a stronger signal to the wireless client. Anyone with suitable equipment can locate a hotspot and take its place using such methods. Evil twins may readily be used to intercept information of a sensitive or personal nature including financial transactions.

While location data hacked in real-time without the consent of individuals is unlikely to be useful for business purposes, there may be some exceptions. According to a Canadian wireless industry consultant, hacking real-time data might prove useful in the case of LBS for fleet management.[140] Citing the example of a taxi company, he noted that location information concerning the whereabouts of vehicles might prove exceptionally valuable to a competitor. Using a similar computer interface they might be able to hack into any taxi fleet management system if user access in not properly validated. The system would need to specify not only that you had access into your company's network of fleet management, but only for that specific list of mobiles. Such safeguards cannot be assumed to be in place. This expert also added that "it is always the case with networks that they are complicated and hard to guard against."[141]

While situations such at the one referred to above are certainly imaginable, it also seems clear that most threats to personal data and location data records will continue to involve the illegal acquisition of information stored in databases. This is a far more universal problem in information-based societies and one that is not peculiar to the case of LBS. Threats in this area are not always posed by hackers. That much was made clear in a recent scandal involving the data collection giant, ChoicePoint. In this incident, personal information on nearly 145 000 people was obtained when individuals posing as legitimate companies were able to gain access to the company's records. Authorities say at least 750 people were defrauded.[142]

---

[138] Connolly, Allison. 2005. "Securing your networks against the risk of rogue wireless access is no longer optional". *ComputerWeekly.com,* January 25, Available: http://www.computerweekly.com.

[139] "'Evil Twin' threat to Wi-Fi users". 2005. *CNN.com*, January 20, Available: http://edition.cnn.com/2005/TECH/internet/01/20/evil.twins/index.html.

[140] Interview: March 7, 2005.

[141] Ibid.

[142] Millard, Elizabeth. 2005. "ChoicePoint Discloses Massive Identity Theft." *CRM Daily*, February 17, Available: http://crm-aily.newsfactor.com/story.

The larger issue of data security has also recently been highlighted in the case of T-mobile. A sophisticated hacker had access to servers of this wireless giant for at least a year. The hacker was able to monitor secret service email, obtain customers' passwords and Social Security numbers, and download candid photos.[143] Technology expert Bruce Schneier argues that the media missed the most important point of the T-mobile incident, which is that data that used to be under people's direct control are now controlled by others. He argues further that the public has little choice but to trust such companies with their privacy, even though the companies have little incentive to protect that privacy. He contends that…

> T-Mobile suffered some bad press for its lousy security, nothing more. It'll spend some money improving its security, but it'll be security designed to protect its reputation from bad PR, not security to protect the privacy of its customers.[144]

In fact, new incentives to address data security issues will likely come from American law-makers. As noted in the *New York Times*, the principle effect of scandals such as those surrounding Choicepoint and T-mobile may be their role in exposing the patchwork of sometimes conflicting state and federal rules that govern consumer privacy in the United States.[145] These and similar incidents involving other data warehousing companies such as LexisNexis could usher in a dramatic reshaping of American privacy laws according to U.S. senator Patrick Leahy.[146] If such scandals continue to occur and to receive extensive coverage in the news, then it also seems likely that pressure to create more explicit legislation in this area will be felt in Canada as well.

Discussion

There is reason to believe that Canadian wireless carriers and service providers will attempt to limit the use of customer location and personal data by third parties without the consent of users. As noted throughout this chapter, the need to head off public privacy concerns has been recognized by corporations hoping to benefit from m-commerce and the provision of LBS. At the same time, there appear to be limits with respect to what an industry may be willing or able to accomplish in terms of curtailing spamming practices, and with respect to larger issues of data security. Problems in the latter area are most likely to arise in relation to the security of personal rather than location information. This issue is not directly related to the provision of LBS. Subscribers to location-based services represent only a tiny portion of those individuals who have made their personal information available to government and commercial organisations. It is the storing of such information in data banks and the potential for its procurement by illicit means which continues

[143] Schneier, Bruce. 2005. *Schneier on Security*. February 14, Available: http://www.schneier.com/blog/archives/2005/02/tmobile_hack.html.
[144] Ibid.
[145] Zeller, Tom Jr. 2005. "Breach Points Up Flaws in Privacy Laws". *The New York Times*. Available: http://www.nytimes.com/2005/02/24/business/24datas.html.
[146] McCullagh, Declan. 2005. "Senator predicts 'overdue' changes to privacy". *News.Com,* March 10, Available: http://news.com/2102-1029_3-5608455.html.

to constitute a privacy threat. However, it is also possible that pressure on relevant Canadian businesses to allocate greater resources in the area of data security may follow in the wake of scandals and legal initiatives south of the border.

Most of the legal issues surrounding the use and procurement of personal information and location data have been framed in the language of consumer consent. However, orientations to privacy which focus on consumer consent and even informed consent must be tempered by the recognition that commerce is actively attempting to shape consumer attitudes over the long-term. While the use of opt-in policies will likely play a growing role in m-commerce, the adoption of such policies must be understood as part and parcel of larger market strategies designed to change the way consumers behave. It should be assumed that such strategies will hold some important and potentially negative consequences for individuals and groups in Canadian society.

As noted by Phillips and Curry,[147] government and corporate bodies have begun to shift their data-collection and delivery mechanisms to cellphones and PDAs which are carried by an individual. One result is that surveillance practices have come more into public consciousness and made privacy issues appear salient. At the same time these researchers argue that:

> because the collection and delivery mechanism is so intimately connected to the body, the focus of those privacy issues has reverted again to the personal affront. The collection and analysis of personal data, and the discriminatory classification of individuals, has taken a back seat to issues of trespass and nuisance.[148]

To better appreciate both the social importance and larger privacy implications of LBS, it is necessary to consider LBS's appearance within the context of existing practices of surveillance and profiling on the part of both government and industry. This is the focus of chapter 5.

[147] Phillips, David & Curry, Michael. 2003. "Geodemographics and the changing spatiality of local practice". In David Lyon (Ed). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Routledge: New York, pg. 147.
[148] Ibid.

Chapter 5

Larger Considerations: Location, Mobility and Privacy in Surveillance Societies

While public opinion may be subject to sudden shifts in the wake of dramatic social or political developments, people in most parts of the world are generally very concerned about the potential abuse of personal information

In this chapter, mobile/location technologies will be considered in terms of their emergence and spread in the form of consumer commodities. Emphasis will be placed on those historic developments which set the stage for their appearance, and the ways in which broader social/cultural and political/economic forces now condition their adoption and use by the public. The purpose of this exercise is to draw attention to the complexity of the influences which presently shape relevant public attitudes, while simultaneously highlighting the potential limitations of approaches to privacy which work mainly within the rubric of individual rights and/or consumer consent. The importance of this dual focus is underscored in the findings of research recently conducted in the United Kingdom. Commenting upon the growth of "mobile ecologies" in Britain, Green and Smith[149] observe that "mobile privatization" has become so commonplace that the population now "takes mobile use, and the data it generates for granted." As a similar mobile landscape takes shape in Canada and elsewhere around the world, it is vital that the implications of this reality continue to be explored.

Over the past few decades, a growing body of research has accumulated concerning public attitudes in the broad areas of surveillance and information privacy. Relevant studies, consisting primarily of survey research, have been conducted in various parts of the world by a wide range of organisations including advocacy groups, government agencies, think tanks, research centres, and commercial and government polling organisations.[150] While the bulk of these surveys have not dealt with mobile/location technologies *per se*, they hold considerable relevance for present purposes. Most importantly, these investigations have consistently revealed that while public opinion may be subject to sudden shifts in the wake of dramatic social or political developments, people in most parts of the world are generally very concerned about the potential abuse of personal information.

Public concerns about information privacy in Canada were made evident in one of the first detailed public opinion surveys concerning privacy conducted in this country. The survey in question, *Privacy Revealed*, was undertaken by EKOS Research in 1993 and was based on a sample of 3 000 Canadians. This study revealed that 90 percent of respondents were generally concerned about privacy issues[151]. In addition, four out of five believed that computers endangered their sense of privacy, 54 percent expressed "extreme" concern over the computer's ability to link personal data stored on several computers, and 60 percent believed that there was less privacy at the time of the survey than during the previous decade. As Zureik[152] observes, *Privacy Revealed* was notable in that it anticipated later developments

[149] Green, Nicola and Smith, Sean. 2004. *Regulation, Information and the Self: Ownership in Mobile Environments (RIS:OME),* pg. 7.
[150] Zureik, Elia. 2004. *Overview of Public Opinion Research Regarding Privacy*, pg. 1.
[151] Zureik, Elia. 2004. *Appendix A: Overview of Public Opinion Research Regarding Privacy,* pg. 10.
[152] Ibid, pg. 11.

in the field of privacy research. For example, the EKOS findings were consistent with a growing body of evidence suggesting that a greater sense of user control over the process of information storage and its release makes people feel more confident that their privacy will not be violated, and that the more transparent the rules are, the less concerned about privacy individuals will be.[153]

Findings commensurate with those cited above were revealed in a four year investigation conducted in the U.K. by the RIS:OME project. The study, *Regulation and the Self: Ownership in Mobile Environments*, which was funded by Intel, was published in January 2004. The project's key findings include evidence that practices of mobile commerce will most likely be successful when organisations maximize the user's control of their own communication information. However, the authors of this study also suggest that increasing user control over personal information is not always a straightforward matter and that "the complexity of relationships between industry and state actors increases the circulation and exchange of mobile data."[154] The relationship(s) which individual citizen/consumers have to larger networks of information over which they may have little control may hold important implications with respect to both public attitudes towards privacy, and the limits of individual autonomy in societies such as Canada. We will return to these points shortly.

Mowshowitz and Zureik[155] suggest that consumer organisations are now "poised to assume the mantle of leadership once held by organized labour" and point out that, in recent years, consumer actions have been associated with a wide range of political agendas and causes. They also observe that in terms of political mobilization, the boycott is perhaps the most powerful weapon in the consumer arsenal. Interestingly, however, despite the growing number of privacy advocacy groups which have appeared in most Western countries, there have been relatively few instances of significant grassroots resistance to corporate or governmental surveillance practices. One notable exception concerns the "Household Marketplace" software advertised by Lotus in 1991. Both consumer and professional groups were concerned by the lack of protection for personal identities offered by this tool along with the fact that Social Security numbers were being used as universal identifiers.[156] In this instance an organisation known as Computer Professionals for Social Responsibility galvanized action through national and international networking. As noted above, however, this incident stands out as a relatively isolated case of popular mobilization over an information privacy concern.

Even a decade ago, Gottlieb[157] maintained that Canadians do not really care much about privacy, but will indicate concern when questioned. He notes that public expressions

[153] Zureik, Elia. 2004. *Appendix A: Overview of Public Opinion Research Regarding Privacy,* pg. 11.
[154] Green, Nicola and Smith, Sean. 2004. *Regulation, Information and the Self: Ownership in Mobile Environments (RIS:OME)*, pg. 5.
[155] Mowshowitz, Abbe and Zureik, Elia. 2004. *Consumer Power in the Digital Society*. University of Minnesota Press: Minneapolis, pg. 4.
[156] Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*, pg. 175.
[157] Gottlieb, Calvin C. 1996. "Privacy: A Concept Whose Time Has Come and Gone". In *Computers, Surveillance & Privacy*. David Lyon & Elia Zureik (Eds.), pp. 156-174.

of anxiety about privacy issues have tended to originate primarily from journalists, lawyers and academics. He contrasts their concern with the glaring lack of attention to privacy matters by politicians, citing this as evidence that the public remains essentially unconcerned about this issue. However, the possibility that members of the public are deeply worried about information privacy issues is not necessarily precluded by a corresponding lack of political action, whether by politicians or by ordinary citizens. As a number of researchers including Lyon[158] and Stalder[159] have suggested, individual responses to privacy issues cannot be adequately appreciated when viewed in isolation from larger social forces. In particular, attention must be given to the role played by social/political and economic systems which have historically been sustained through shifting practices of surveillance. Gandy[160] gets to the heart of the matter when he observes that "when individuals must supply personal information in order to acquire goods and services in the market, they are responding to a form of power."

When attempting to conjoin the issue of public attitudes to privacy with the reality of location technology proliferation, it is important to consider each in relation to longer-term historic trends. In particular, attention must be given to both the development of modern surveillance practices on the part of state and the gradual shift from production-based to consumer-based capitalism in North America and elsewhere. One need only briefly consider the hybrid character of mobile/location technologies to appreciate the relevance which developments in both of these closely related areas hold. For example, the technical integration of devices such as cellphones, Wi-Fi internet and personal digital assistants (PDAs) within larger GPS networks would not be possible without the existence of orbital satellites originally deployed for military purposes by the American government. At the same time, these mobile technologies represent a new class of personalized mass commodities, the effective marketing of which depends upon the continuous application of increasingly sophisticated consumer profiling practices. In fact, overlapping concerns relating to surveillance and privacy converge at numerous points within and between the public and private spheres, as the remaining discussion will hopefully make clear.

As Lyon[161] has observed, attempts to monitor and regulate the size, constitution, and activities of human populations, may be traced to ancient times. Upon reflection, this fact is perhaps unsurprising. It has long been recognized by social scientists that when the size and boundaries of communities become too large or undefined for their members to communicate and exchange goods with one another directly

[158] Lyon, David. 2001. *Surveillance Society*. Open University Press: Philadelphia, pp. 134-135.
[159] Stalder, Felix. 2002. "Privacy is not the antidote to surveillance", *Surveillance & Society*, Vol. 1, No. 1, pp. 120-124, Available: www.surveillance-and-society.org.
[160] Gandy, Oscar H. Jr. 1996. "Coming to Terms with the Panoptic Sort". In *Computers, Surveillance & Privacy*. David Lyon & Elia Zureik (Eds.), University of Minnesota Press: Minneapolis, pg. 145.
[161] Lyon, David. 2003. *Surveillance after September 11*. Polity: Cambridge, pg. 24.

or on a regular basis, increasingly impersonal and indirect mechanisms must be established to allow for the continued possibility of large-scale social integration. In fact, the appearance of civilizations in the form of heavily populated settlements supported by intensive agriculture have invariably been marked not only by the introduction of increasingly abstract means of economic and legal/governmental integration, but also by the emergence of social classes and information specialists entrusted with their effective management.[162] However, it wasn't until the relatively recent appearance of nation/states beginning in the late 1700s that practices of census taking, record keeping, and other forms of social surveillance developed on a scope and scale which distinguishes modern societies both from their predecessors and from other existing forms of collective social life.

The "imagined community" of the contemporary nation-state would not have been realizable without dramatic developments in the area of mass communication, and without large-scale practices of government administration.[163] Clearly, the organizing power of the state and its institutions was a necessary precondition for the rise of industrialized mass societies in the United States and Canada from the early twentieth century onwards. In addition to regulating the economy and facilitating trade, the state was responsible for mobilizing vast human and material resources in the areas of public education, military service, policing, health care and social welfare. Collectively, these practices were necessary both to maintain the state's internal and external security and to establish the legitimacy of government institutions by guaranteeing fundamental rights to citizens. With the advent of the information revolution starting from roughly the 1970s onwards, the state's capacity to maintain public order, police its borders and serve the needs of citizens increased dramatically. We will return to the last point shortly.

Significantly, the growth of state bureaucracies during the twentieth century was paralleled by similar developments in the private sector. The gradual progression from a production-based to a more consumer-driven economy went hand-in-hand with the rise of monopoly capitalism. Much like the modern state, the capitalist enterprise became increasingly dependent upon the activity of clerical and information workers and the efficient storage of information. During roughly the first half of the century, profits were guaranteed by the saturation of mass markets with standardized goods. Eventually, however, consumer demands for ever more novel and customized commodities could not be adequately addressed through traditional assembly line forms of production.[164] It is now widely accepted that the development of digital technology and the subsequent computerization

[162] Harris, Marvin. 1978. *Cannibals and Kings: The Origins of Cultures.* Vintage Books: New York.
[163] Anderson, Benedict. 1991. *Imagined Communities: Reflections on the Origins and Spread of Nationalism*. Verso: New York.
[164] Slater, Don. 1997. *Consumer Culture and Modernity*. Polity: Cambridge, pp. 183-188.

of the workplace were necessary preconditions for the shift to a more flexible form of capitalism, one capable of meeting the challenge of a consumer-driven economy.

The increasing computerization of the workplace has allowed more flexible forms of commodity production to displace older Fordist modes of mass assembly. It is largely the ability to rapidly re-tool and re-program the production process which has enabled the post-Fordist enterprise to remain viable. Small batches of customized goods may now be produced to contend with both the rapid growth of consumer niche markets, and equally rapid changes in consumer tastes. At the same time, new market segments must continuously be identified and created through increasingly sophisticated marketing practices.[165] This new emphasis on flexibility has in turn relied upon new forms of information exchange within the workplace, including new forms of employee surveillance.

In the idealized post-Fordist corporation, employees work in loose networks where responsibility and information flows are far more evenly dispersed throughout the overall enterprise. However, the notion that the new workplace empowers ordinary workers by involving them more directly in decision making and creative forms of work remains contested. While information workers such as computer programmers arguably engage in relatively creative work and enjoy a degree of autonomy made possible by their expertise, this is less likely to be the case for most employees in contemporary work settings. Not coincidentally, the appearance of new forms of workplace surveillance has provided a catalyst for recent debates concerning the empowerment vs. disempowerment of flexible and/or mobile workers.[166]

New forms of electronic monitoring are now entrenched in most modern work settings. Some examples of mobile worker monitoring via location technologies were discussed in chapter 4. Ethical concerns already raised by older practices of workplace surveillance have arguably become more pronounced have as a result of electronic monitoring. As Marx points out, "if we draw a parallel between the information gathering net and a fishing net, then the mesh of the net has become finer and the net wider."[167] As suggested in chapter 4, this reality may result in more intense scrutiny of workers and greater discrimination. However, other related points are worth raising here as well. For example, Marx also observes that entrenched cultural beliefs may also serve to legitimate surveillance practices. Attitudes such as "I have nothing to hide," "It's the way they do things around here" or "I'm getting paid" may mask oppressive conditions in the workplace and within society at large.[168] It

[165] Slater, Don. 1997. *Consumer Culture and Modernity*. Polity: Cambridge, pp. 183-188.
[166] Zureik, Elia. 2003. Theorizing Surveillance: The Case of the Workplace. (pp. 31-56) In, David Lyon (ed.). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. pg. 46.
[167] Marx, Gary T. 1999. "Measuring Everything That Moves: The New Surveillance at Work". In Research in the Sociology of Work. 9. (165-189). Eds. I. Simpson & R. Simpson. Stamford: Jai Press Inc. pg. 166.
[168] Marx, Gary T. 2003. "A Tack in the Shoe: Neutralizing and Resisting Surveillance". *Journal of Social Issues*. 59 (2). (165-189) pg. 370.

should also be emphasized that increased workplace surveillance has arisen in conjunction with other political/economic trends which may exacerbate its negative effects. The latter include increasing global market competition and the declining power of unions.[169]

In addition to internal changes to the workplace, greater and more efficient integration among corporations, suppliers of resources, and financial institutions have been enabled by the rapid development of computer networking capabilities. Significantly, the same information technologies which allowed for more flexible forms of capitalism at home, and more fine-grained monitoring of employees, have also contributed to the rise of the global economy. Castells[170] maintains that the global economy is distinct from earlier world economies due to the fact that its core components "have the institutional, organisational, and technological capacity to work as a unit in real time, or chosen time, on a planetary scale." The resulting complex of overlapping commercial networks within and across the borders of states has necessarily been accompanied by massive international flows of capital, information and labour.

One result of these changes is that new incentives have arisen on the part of governments for identifying, profiling and monitoring increasingly mobile and heterogeneous populations. Lyon[171] and others have discussed these changes with respect to the welfare state's displacement by the safety-and-security state. One of the safety-and-security state's defining characteristics is a preoccupation with the control of risk. This preoccupation has led to a corresponding dependence upon digital communication and information technologies (CITs), which have become indispensable for providing real-time data and allowing for the storage and flow of information on a scale previously unimaginable. Taken together, these changes in political orientation and technological development may have negative consequences for certain groups in countries such as Canada. For example, Canada's Bill C-36 extends the definition of terrorism to include those "who intend to cause serious interference with or serious disruption of an essential service," and permit a minister to compile a list of "terrorist groups."[172] As Lyon has made clear, such broad definitions invite the potential for serious abuse.[173]

The growth of transnational commerce combined with the regulation of trade and investment by international monetary organisations have reduced corporate vulnerability to environmental, trade and labour regulations as well as to restrictions of currency exchange formerly imposed by governments.[174] Conversely, states have felt increasingly compelled to respond more favourably to the

[169] Wood, Anne Marie. 1998. "Omniscient Organisations and Bodily Observations: Electronic Surveillance in the Workplace." *International Journal of Sociology and Social Policy*. 18(5/6). pp.132-169.
[170] Castells, Manuel. 2004. *The Power of Identity*. Blackwell: Oxford, pg. 102.
[171] Lyon, David. 2003. *Surveillance after September 11*. Polity: Cambridge.
[172] Ibid. pg. 50.
[173] Ibid.
[174] Castells, Manuel. 2004. *The Power of Identity*. Blackwell: Oxford, pp. 312-316.

demands of commercial enterprise, particularly with respect to taxation and greater pressure to privatize areas such health care which were formerly kept within the public domain. A relevant example may be seen with respect to the CRTC's 1997 decision not to regulate the internet. In essence, this decision led to a transfer of the regulator's role from the Canadian government to a shrinking handful of increasingly powerful Internet Service Providers.[175] Significantly, this transfer has resulted in less rather than more freedom on the part of most internet users to influence Web content. At the same time, ISPs have been allowed not only to play the role of censor, but also to place constraints on the ways in which the Web may be navigated and used for purposes of communication. Ordinary users are now encouraged to approach the Web as a read-only medium.[176]

The CRTC's decision not to regulate the internet holds significance when considered in conjunction with the evolving reality of media convergence. Traditionally, a clear distinction between broadcast media (television and radio) and communication media (telephony) underpinned government policies concerning the appropriate relationship between carrier and content in each case.[177] With respect to broadcast media, the Canadian government has long reserved the right to regulate content in the service of the public, and in a manner which ostensibly safeguards Canadian identity. Conversely, in the case of telecommunications, carriers such Bell Canada have historically had no right to exercise influence over communication content, which is provided entirely by users of the service. These developments may take on future importance in the case of technologies such cellphones and PDAs, which, like the internet, represent hybrids of broadcast and telecommunications technologies. As the Canadian public is gradually conditioned to be more accepting of LBS and practices of m-commerce, the CRTC may well come under renewed pressure to modify existing policy frameworks to be more responsive to changing public attitudes and new technological realities.

As previously indicated, both governments and corporations are now highly dependent upon electronic networks and databases to keep tabs on the habits and whereabouts of individuals and groups in society. The crucial point here is not that Big Brother is watching our every move, but rather that in contemporary information societies, surveillance has become synonymous with social sorting. As Lyon summarizes:

> Surveillance has to be understood today as social sorting, which has exclusionary consequences. Watching others has become systematic, embedded in a system that classifies according to certain pre-set criteria, and sorts into categories of risk

[175] Winseck, Dwayne. 2001. "Netscapes of Power: Convergence, Network Design, Walled Gardens and Other Strategies of Control in the in the Information Age". In, David Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. pp.176-198.
[176] Ibid.
[177] Ibid.

> and opportunity. These categories in turn relate to suspicion or to solicitation – and many purposes in between – depending on the purposes for which the surveillance is done.[178]

Understanding surveillance practices in terms of social sorting helps to highlight the limitations of viewing privacy exclusively through reference to individual rights, or even with respect to individual perceptions and attitudes. Often, the information gathered for surveillance purposes is not personal information at all, and the processes through which it gains value to governments or marketers remain invisible to most members of the public. Referring to modern surveillance practices in the terminology of a "panoptic sorting machine" Gandy observes that:

> when personal information about individuals is combined with similar information about other individuals, the goal is frequently the generation of information about countless others whose behavior has not been directly measured. The panoptic technology is an *inferential* difference machine. Its predictions are based on information gathered from sample of their behaviors. Information gathered from particular individuals is frequently most useful in developing approaches to *other* individuals who may remain unknown to the organisation until they respond to a promotional appeal.[179]

Danna and Gandy[180] observe that by using analytical and personalized software, businesses can determine what an individual's needs are based on the profile into which the customer fits. The customer is then provided with a product or service that meets those needs. Significantly, the same logic underpins the recent development of LBS in the United States. As noted by Curry, Phillips and Regan[181] both LBS and E-911 make use of a technical paradigm within which the location of individuals is mapped in real-time, and within which the system may incorporate additional information about the individual, including demographic characteristics and past behaviour. Hence, LBS practices which make use of aggregate data for marketing purposes are best understood as part and parcel of a larger trend in which public information may profitably be merged with private computing resources to better divide the landscape into discrete spaces occupied by homogenous groups of households and individuals.[182]

Clearly, mobile technologies, such as cellphones, PDAs and Wi-Fi internet, and RFID tags in conjunction with the network infrastructures and computer databases to which they are either directly or indirectly linked, offer greater visibility and transparency with respect to the movements and habits of consumers, workers, prisoners, patients, and children among others. At the same time, the

[178] Lyon, David. 2003. *Surveillance after September 11*. Polity: Cambridge, pg. 149.
[179] Gandy, Oscar H. Jr. 1996. "Coming to Terms with the Panoptic Sort". In *Computers, Surveillance & Privacy*. David Lyon & Elia Zureik (Eds.), University of Minnesota Press: Minneapolis, pg. 140.
[180] Danna, Anthony & Gandy, Oscar H. Jr. 2002. "All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining". *Journal of Business Ethics*, Vol. 40, pg. 377.
[181] Curry, Michael R., Phillips, David J. and Regan, Priscilla M. 2004. "Emergency Response Systems and the Creeping Legibility of People and Places". *The Information Society*, Vol. 20, pg. 367.
[182] Phillips, David & Curry, Michael. 2003. "Privacy and the Phenetic Urge: Geodemographics and the changing spatiality of local practice". In *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. In, David Lyon (ed.), pg. 137.

aggressive promotion of these personalized devices by industry fits well with the liberal market philosophy of individual freedom of choice. The liberating capacity of the cellphone is regularly celebrated in advertising. Cellphones and related products such as PDAs have ostensibly been tailored to meet the needs of independent, mobile citizens who presumably desire greater freedom and flexibility at work and play. And yet, as emphasized throughout this chapter, industry's capacity to both create and address the needs of mobile consumers is predicated on a feedback loop through which the ability to control ever more aspects of public and private life continues to increase.

Returning to the matter of public attitudes, we may now better appreciate that approaches to information privacy focussing primarily on questions of individual or consumer consent, and even of informed consent, may be less adequate than might at first appear to be the case. As Stalder[183] observes, from the standpoint of the individual, making dozens of complex decisions each day about which data collection to consent to and which to refuse is clearly impractical. Living up to such an ideal of "informational self-determination" simply demands too high a price in terms of cognitive overload. Stalder[184] also draws attention to the individual's constitution as a nodal point within information networks wherein the possibility of disconnection is highly undesirable. For example, he points out that when renting a car anywhere in the world one does not need a passport, the traditional stable identifier, but rather a credit card. This card expresses nothing more than the individual's relationship to a bank. It does not indicate who one is, but whether one can be trusted. Following this logic further, Stalder[185] argues that when important aspects of identity shift form stable identifiers such as nationality to dynamic relationships such as credit rating, notions of separation become unworkable.

Given the choice between adopting technologies and new services ostensibly designed to enhance one's material and social success, and obsessing over relatively abstract considerations of personal privacy, it is perhaps unsurprising that many or most citizens/consumers will continue to opt for the former. However, as Lyon makes clear, approaching privacy issues from the vantage point of networks and social sorting in no way detracts from its social/political importance:

> How persons are "made up" by surveillance systems, and with what consequences, is a vital question. If the "data double" that circulates through electronic systems does help to determine what sorts of treatment we receive from insurance companies, the police, welfare departments, employers, or marketing firms, then it is far from an innocent series of electronic signals.[186]

[183] Stalder, Felix. 2002. "Privacy is not the antidote to surveillance." *Surveillance & Society*, Vol. 1, No. 1, Pg. 122.
[184] Ibid.
[185] Ibid.
[186] Lyon, David. 2003. *Surveillance after September 11*. Polity: Cambridge, pg. 149.

These points are significant and emphasize the need to approach issues of surveillance and privacy not only with respect to individual rights or the invasion of personal space, but also with a mind to the roles ideally played by individuals and groups in a democratic society. Ultimately, concepts such as privacy and democracy can only remain meaningful if people and communities are able to exercise their capacity to make choices which have lasting consequences for society as a whole. This includes the freedom not only to select brand X over brand Y, but also to gain greater control over the institutions and the information/communication networks which increasingly define their social/political environment.

Chapter 6
Future Directions: Social Research and Public Policies

Social Science Research

Survey research in the area of public attitudes to privacy continues to accumulate. Future research should include qualitative as well as quantitative approaches to understanding collective and individual attitudes to privacy and surveillance. More research is still needed to shed greater light o the following interrelated areas:

- The role played by a range of variables in affecting attitudes to privacy including gender, cultural variables (religion, ethnicity etc.), nationality, and previous exposure to information technologies

- The role played by government and corporate policies, as well as public relations campaigns, aimed at winning greater public acceptance of location technologies in affecting citizens' attitudes

- The role of the popular media in affecting attitudes to location technologies

- The relationship between attitudes and political activism (for example between negative attitudes concerning the use of location technologies in various environments such as the workplace and possible responses in the form of collective action)

- Comparative studies of location technologies, particularly in countries with fairly dense urban populations and already existing widespread use of cellphones such as Finland and Japan

Note: Many of these issues are now being explored at length in the Globalization of Personal Data Project, as well as in several related research projects in Canada and elsewhere.

Additional Social Science and Practical Research

To complement the research directions listed above, further investigation into the following areas would also be helpful:

- The accuracy of predictions about relevant business/technology developments made by marketing research organisations such as Gartner, Forrester, Giga, Budde, etc.

- Closer attention to the vulnerabilities of data storage and management in both the private and public sectors, including location data

- Closer attention to issues of media convergence, particularly in light of traditional government policy approaches to various mass media and communications media

Public Policy

In recent years, numerous recommendations have been made by industry associations, legal experts and others concerning appropriate government policies in the area of personal/information privacy. Throughout much of this report, emphasis has been placed upon the larger issue of surveillance and its relationship to corporate and government practices of social sorting. Clearly, this reflects our social research interests in relation to historic practices of governance, ideology and social change. However, we also believe that closer attention to social sorting practices may have a positive impact upon privacy policy formulation. In particular, addressing privacy issues arising in relation to the use of anonymous aggregate data would help to balance the present emphasis placed upon individual privacy controls and rights as they relate to PIPEDA. Further

consideration could be given to the following derivative concerns with respect to policy formulation:

- The possibly unrealistic expectation that consumers/citizens will be guided in their actions/choices by ideals of informational self-determination and recognition that the recent introduction of location technologies and LBS add to the complexities of the information landscape

- That an individual's acceptance or rejection of particular policies, services or information practices, such as those surrounding LBS, is not simply a matter of choice, but also reflects existing power relationships

- That opt-in policies and ideals of informed consent, while important and desirable in many cases are also only useful with respect to certain types of privacy concerns. Anonymous, aggregate location data, much like aggregate personal data, may be highly valuable to marketers

- The interdependence between government policies, corporate marketing strategies and popular attitudes to privacy when considering public acceptance of rejection of LBS

Finally, with respect to all of the concerns raised above, it seems appropriate that relevant policies should be formulated at the most general level to cover whatever specifics are thrown up by the development of new technologies and the manner in which they are adopted by end-users.

Glossary

The **Angle of Arrival (AOA)** method of locating a wireless caller (see figure 4 on page 18) is just one of several that may be selected by wireless carriers to meet Enhanced 911 Phase II requirements by October 2001. The Time Difference of Arrival (TDOA), location pattern matching and GPS methods are also being considered. There are also hybrid location methods that use both TDOA and AOA technology. The TDOA, AOA and location pattern matching methods are network based, while the GPS method is handset based.

Using this technique:

- A wireless subscriber can use any handset (digital, analog, TDMA, CDMA, no special add-ons) to make a 911 call.
- The wireless phone's signal is received at various antenna sites. Each antenna site is equipped with additional gear to detect the compass direction from which the caller's signal is arriving. Generally, at least three sites must receive the handset signal to provide an accurate location.
- The receivers send the caller's voice call and compass data to the mobile switch, where the angles are compared and computed to generate a latitude and longitude for the caller.
- The caller's voice call and the latitude and longitude are then sent to the PSAP for use by the dispatcher.

Further information about AOA location technology can be found at the following web address: http://www.911dispatch.com/911_file/aoa.html.

Anonymity ensures that subjects may use a resource or service without disclosing their user identities. Requirements for anonymity provide protection of the user identity. Note that anonymity is **not** intended to protect the subject identity. Anonymity is intended to specify that a user or subject might take action without releasing its user identity to other users, subjects or objects.

The **Anti-Terrorism Act** is one of several pieces of legislation that form the Government of Canada's overall anti-terrorism strategy. It takes aim at terrorist organisations and assists the Government of Canada in meeting the extraordinary challenges that terrorism poses. The legislation was intended to protect the safety, security and fundamental rights of Canadians. It contains numerous safeguards, which include an important requirement that Parliament comprehensively review the provisions and operation of the Act after three years.

The *Anti-terrorism Act* provides new investigative tools to security, intelligence and law enforcement agencies to ensure that the prosecution of terrorist offences can be undertaken efficiently and effectively.

One measure is the investigatory power already in the *Criminal Code* that makes it easier to use electronic surveillance against criminal organisations where applied to suspected terrorist groups. This includes eliminating the need to demonstrate that electronic surveillance is a last resort in the investigation of terrorists, which affects the level of control that ISPs and telecom carriers have over protecting their customers' identities and personal data communications.

Additionally, the period of validity of a wiretap authorization was extended from 60 days to up to one year when police are investigating a terrorist group offence. As a further measure, the requirement to notify a target after surveillance has taken place can be delayed for up to three years. A Superior Court judge still has to approve the use of electronic surveillance to ensure that these powers are used appropriately.

A **Carrier service provider** is a company offering telephone and data communications between points in a state or in one or more countries. The *Regional Bell Operating Companies (RBOCs)* are an example of carriers.

A **Carrier signal** is a frequency in a communications channel modulated to carry analog or digital signal information. For example, an FM radio transmitter modulates the frequency of a carrier signal and the receiver processes the carrier signal to extract the analog information. An AM radio transmitter modulates the amplitude of a carrier signal.

A **Carrier system** is a communications system providing a number of point-to-point channels through some type of multiplexing. T-1 and T-3 carrier services are examples of carrier systems that can be used between points in a Wide Area Network (WAN).

Code Division Multiple Access (CDMA) is a method for describing physical radio channels. Data intended for a specific channel are modulated with that channel's code. These are typically pseudorandom in nature, and possess favourable correlation properties to ensure physical channels are not confused with one another.

Cell of Origin (COO) is a mobile positioning technique for finding a caller's cell (the basic geographical coverage unit of a cellular telephone system) location. It may be used by emergency services or for commercial use. COO is the only positioning technique that is widely used in wireless networks and is used for Phase I of E-911 services in the U.S.

For COO positioning, the location of the base station is ascertained and considered to be the location of the caller. COO is a variable and not a very precise locator; depending on the number of base stations in the search area, the measure may be accurate to within 100 metres of the target (in an urban area) or as far off as 30 kilometres away from the target where base stations are less densely concentrated. For this reason, when precision is important COO is often used in conjunction with some other technology, such as the Global Positioning System (GPS) or Time of Arrival (TOA).

Although COO positioning is not as precise as other methods, it offers unique advantages: it can very quickly identify the location (generally in about three seconds) and does not require equipment or network upgrades, which makes it easily deployed to existing customer bases. The American National Standards Institute (ANSI) and the European Telecommunications Standards Institute (ETSI) recently formed the T1P1 subcommittee dedicated to creating standardization for positioning systems using TOA, Assisted GPS, and Enhanced Observed Time Difference (EOTD) in addition to COO.

Confidentiality is the controlled release of personal information to an information custodian under an agreement that limits the extent and conditions under which the information may be used or released further.

Data Minimization or **Data Scarcity** ensures that a subject's personal data is limited in quantity while collecting, storing, using and sharing with third parties. This principle ensures that limited profiles are kept of the data subject throughout a system or service provision.

Encryption is the translation of data into a secret code. It is currently the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

Enhanced 911 (E-911) is a location technology advanced by the Federal Communications Commission (FCC) that will enable mobile, or cellular, phones to process 911 emergency calls and enable emergency services to locate the geographic position of the caller. When a person makes a 911 call using a traditional phone with ground wires, the call is routed to the nearest public safety answering point (PSAP) that then distributes the emergency call to the proper services. The PSAP receives the caller's phone number and the exact location of the phone from which the call was made. Prior to 1996, 911 callers using a mobile phone would have to access their service providers in order to get verification of subscription service before the call was routed to a PSAP. In 1996 the FCC ruled that a 911 call must go directly to the PSAP without receiving verification of service from a specific cellular service provider. The call must be handled by any available service carrier even if it is not the cellular phone customer's specific carrier. Under the FCC's rules, all mobile phones manufactured for sale in the United States after February 13, 2000, that are capable of operating in an analog mode must include this special method for processing 911 calls.

The FCC has rolled out E-911 in two phases. In 1998, Phase I required that mobile phone carriers identify the originating call's phone number and the location of the signal tower, or cell, accurate to within a mile. In 2001, Phase II required that each mobile phone company doing business in the United States must offer either handset-based or network-based location detection capability so that the caller's location is determined by the geographic location of the cellular phone within 100 metre accuracy and not the location of the tower that is transmitting its signal. The FCC refers to this as Automatic Location Identification (ALI).

Enhanced Observed Time Difference (EOTD) uses up to four different cellular base stations to figure out a cellphone's location, measuring the arrival times of the call at various different cellular antennas. But in rural areas, cellular base stations are sometimes miles apart. Instead of four, it's likely there will be just two base stations to help figure out the location, which makes it less accurate.

Global Positioning System (GPS) is a worldwide Middle Earth Orbit satellite navigational system formed by 24 satellites orbiting the earth and their corresponding receivers on the earth (see diagram on page 15). The satellites orbit the earth at approximately 19 000 kilometres above the surface and make two complete orbits every 24 hours. The GPS satellites continuously transmit digital radio signals that contain data on the satellites' locations and the exact times to the earth-bound receivers. The satellites are equipped with atomic clocks that are precise to within a billionth of a second. Based on this information the receivers know how long it takes for the signal to reach the receiver on earth. As each signal travels at the speed of

light, the longer it takes the receiver to get the signal, the farther away the satellite is. By knowing how far away a satellite is, the receiver knows that it is located somewhere on the surface of an imaginary sphere centered at the satellite. By using three satellites, GPS can calculate the longitude and latitude of the receiver based on where the three spheres intersect. By using four satellites, GPS can also determine altitude.

GPS was developed and is operated by the U.S. Department of Defense. It was originally called NAVSTAR (Navigation System with Timing and Ranging). Before its civilian applications, GPS was used to provide all-weather round-the-clock navigation capabilities for military ground, sea, and air forces.

GPS has applications beyond navigation and location determination. It can be used for cartography, forestry, mineral exploration, wildlife habitation management, monitoring the movement of people and things and bringing precise timing to the world.

Global System for Mobile Communications (GSM) is one of the leading digital cellular systems. GSM uses narrowband Time Division Multiple Access (TDMA), which allows eight simultaneous calls on the same radio frequency.

GSM was first introduced in 1991. As of the end of 1997, GSM service was available in more than 100 countries and has become the *de facto* standard in Europe and Asia.

A **hotspot** is a specific geographic location in which an access point provides public wireless broadband network services to mobile visitors through a WLAN. Hotspots are often located in heavily populated places such as airports, train stations, libraries, marinas, conventions centres and hotels. Hotspots typically have a short range of access.

An **Internet Service Provider (ISP)** is a company that provides access to the internet. For a monthly fee, the service provider gives you a software package, username, password and access phone number. Equipped with a modem, you can then log-on to the internet and browse the World Wide Web and USENET, and send and receive email.

In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company's networks to the internet. ISPs themselves are connected to one another through Network Access Points (NAPs).

Lawful interception (aka wiretapping) of telecommunications is the interception of telecommunications by law enforcement authorities (LEAs) and intelligence services, in accordance with local law and after following due process and receiving proper authorization from competent authorities. Various countries have different rules with regards to lawful interception. In the U.S., the law is known as Communications Assistance for Law Enforcement Act (CALEA).

Location-based Services (LBS) are a relatively new generation of tracking devices and their applications. It is unique because it provides the ability to seek out a geographical location device or receiver, in some cases with pinpoint accuracy. Location technology is also unique because it allows for continuous and therefore real-time tracking of a device. Although such capabilities exist, commercial

application of such real-time, continuous location tracking have been viewed by many potential service providers and users as costly, invasive, unnecessary and/or extremely resource dependent. As a result, location technology is most commonly deployed either through a wireless handset that has an embedded chip, which communicates with other handsets, satellites and cell sites or through a network of cell-sites or base stations alone.

Location Pattern Matching (LMP) method of locating a wireless caller is just one of several that may be selected by wireless carriers to meet Phase II requirements by October 2001. The Angle of Arrival entry on page18 outlines some of the other methods being considered for E-911 and other applications.

Using this technique:

- A wireless subscriber can use any handset (digital, analog, TDMA, CDMA, no special add-ons) to make a 911 call.
- The wireless phone's signal is received at various antenna sites equipped with special gear.
- The receivers send the caller's voice call to the mobile switch, where sophisticated equipment analyzes the acoustic radio signal, and then compares it to a database of standard signal characteristics. These characteristics include signal reflections (multipath), echoes and other signal "anomalies." According to U.S. Wireless, the only supplier of gear for this technique, when a computerized match is made, the location of the caller can be determined within the FCC's requirements. The technique is effective in urban environments that include tall buildings and other obstructions, where other techniques might not succeed.
- The caller's voice call and the latitude and longitude are then sent to the PSAP for use by the dispatcher. (http://www.911dispatch.com/911_file/lpm.html)

Medium or Middle Earth Orbit (MEO) is a satellite system used in telecommunications. MEO satellites orbit the Earth between 1 600 and 35 900 kilometres above the Earth's surface. MEOs are mainly used in geographical positioning systems and are not stationary in relation to the rotation of the Earth.

An **overlay network** is a type of network architecture, usually referring to one network running on top of another. For example, peer-to-peer networks are usually overlay networks because they run on top of the internet.

The overlay contains the distributed information in the network including connectivity information, location/name of superpeers, closest peers, and adjacency. Dial-up internet is essentially an overlay upon the traditional telephone network.

Peripherals are types of computer hardware that are added to a host computer in order to expand its abilities. More specifically the term is used to describe those devices that are optional in nature, as opposed to hardware that is either demanded or always required in principle.

The term also tends to be applied to devices that are hooked up externally, typically though some form of computer bus like USB. Typical

examples include joysticks, printers and scanners. Devices such as monitors and disk drives are not considered peripherals because they are not truly optional, and video capture cards are typically not referred to as peripheral because they are internal devices.

PDA Personal Digital Assistant. A handheld device that combines computing, telephone/fax, Internet and networking features.

Personal Information Protection and Electronic Documents Act (PIPEDA) is the Canadian Act in effect since January 2001 to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act. This Act differs from Canada's Privacy Act in that it covers private sector privacy practices and compliance. See http://laws.justice.gc.ca/en/P-8.6/92607.html

Privacy is the right and/or desire of a person to control the access, use and disclosure of personal information.

A **Public Safety Answering Point (PSAP)** is a physical location where 911 emergency telephone calls are received and then routed to the proper emergency services.

Pseudonymity ensures that users may use a resource or service without disclosing their user identities, yet still be held accountable for their use. While pseudonymity resembles anonymity in that they both protect the identity of the user, pseudonymity maintains a reference to the user's identity for accountability or other purposes.

Radio Frequency Identification (RFID) is a technology similar, in theory, to bar code identification. With RFID, the electromagnetic or electrostatic coupling in the RF portion of the electromagnetic spectrum is used to transmit signals. An RFID system consists of an antenna and a transceiver that read the radio frequency and transfer the information to a processing device, and a transponder, or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted.

RFID systems can be used just about anywhere, from clothing tags to missiles to pet tags to food, anywhere that a unique identification system is needed. The tag can carry information as simple as a pet owner's name and address to instructions as complex as how to assemble a car. Some auto manufacturers use RFID systems to move cars through an assembly line. At each successive stage of production, the RFID tag tells the computers what the next step of automated assembly is.

One of the key differences between RFID and bar code technology is RFID eliminates the need for line-of-sight reading that bar coding depends on. Also, RFID scanning can be done at greater distances than bar code scanning. High frequency RFID systems (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) offer transmission ranges of more than 27 metres although wavelengths in the 2.4 GHz range are absorbed by water (the human body) and therefore have limitations.

RFID is also called Dedicated Short Range Communication (DSRC).

Security, in the computer industry, refers to policies, procedures and safeguards used for ensuring that data stored in a computer cannot be read or compromised by any individual without authorization. Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

SMS Short Message Service. A service for sending short text messages to mobile phones.

Time Division Multiple Access (TDMA) is a technology for delivering digital wireless service using time-division multiplexing (TDM). TDMA works by dividing a radio frequency into time slots and then allocating slots to multiple calls. In this way, a single frequency can support multiple, simultaneous data channels. TDMA is used by the GSM digital cellular system.

The **Time Difference of Arrival (TDOA)** method of locating a wireless caller (see figure 5 on page 19) is just one of several that may be selected by wireless carriers to meet Phase II requirements by October 2001. The Angle of Arrival entry on page 18 outlines some of the other methods being considered for E-911 and other applications. This technique is used by True Position in their Phase II products.

Using this technique:

- A wireless subscriber can use any handset (digital, analog, TDMA, CDMA, no special add-ons) to make a 911 call.
- The wireless phone's signal is received at various antenna sites. Since each antenna is (usually) a different distance from the caller, the signal arrives at a (very) slightly different time. The technique requires signal timing information from at least three different antenna sites.
- The receivers, synchronized by an atomic clock, send the caller's voice call and timing data on to the mobile switch, where the times are compared and computed to generate a latitude and longitude for the caller.
- The caller's voice call and the latitude and longitude are then sent to the PSAP for use by the dispatcher.

Further information about TDOA location technology can be found at the following web address: (http://www.911dispatch.com/911_file/tdoa.html)

Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together. Unlinkability differs from pseudonymity because, while users do not know the identity of another user with pseudonymity, they can discover the links between different actions the user has taken.

Unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used. Unobservability approaches the user identity from a different direction than unlinkability. In

this case, the intent is to hide the use of a resource or service, rather than to hide the user's identity.

WAN Wide Area Network.

WLAN Wireless Local-Area Network. Also referred to as *LAWN*.

Wardrivers are people who participate in an activity that consists of driving around with a Wi-Fi-equipped computer, such as a laptop or a PDA, in one's vehicle, detecting Wi-Fi wireless networks. It is also known (as of 2002) as "WiLDing" (Wireless LAN Driving) and originated in the U.S. with the Bay Area Wireless Users Group (BAWUG). It is similar to using a scanner for radio. Many wardrivers will use GPS devices to measure the location of the network find and log it on a website. For better range, antennas are built or bought, and vary from omnidirectional to highly directional. Software for wardriving is freely available on the internet, notably, NetStumbler for Windows, MacStumbler for Macintosh, and Kismet for Linux. Wardriving was named after Wardialing because it also involves searching for accessible computer systems. The average wardriver is typically only out to log and collect information from the Access Points (APs) they find while driving.

In the U.S. accessing a communications network without authorization is illegal. The law differs in other countries. For example, a wardriver in the U.K. might be caught with the "use of a computer for a purpose for which you do not have permission" clause. This is a commonly misunderstood concept. Wardrivers do not, in fact, usually use services without authorization and may not even transmit a signal at all.

Wi-Fi is the wireless way to handle networking. It is also known as 802.11 networking and wireless networking. The big advantage of Wi-Fi is its simplicity. You can connect computers anywhere in your home or office without the need for wires. If you are travelling you will be able to access nodes or hotspots that are also being built so that your wireless laptop can connect up to a whole network along your route (eg. VIA Rail has hotspots built into their first-class rail cars). The computers connect to the network using radio signals, and computers can be up to 30 metres or so apart.

The radios used in Wi-Fi are not so different from the radios used in $5 walkie-talkies. They have the ability to transmit and receive. They have the ability to convert 1s and 0s into radio waves and then back into 1s and 0s.

Terms have been taken from the following on-line technical dictionaries:

Wikipedia:
http://en.wikipedia.org/wiki/Main_Page
Webopedia:
http://www.webopedia.com/
The CDT's Guide to Online Technology:
http://www.cdt.org/privacy/guide/terms/
Location based services definitions are found at: http://www.911dispatch.com

Bibliography

A Brave Mobile World: Emerging Technologies for Mobility. 2001. T-14-0297, Gartner Inc., October 1.

"Accuracy is Addictive" 2002. *The Economist.com,* March 14, Retrieved: January 24, 2005, Available: http://www.economist.com/PrinterFriendly.dfm?Story_ID+1020779.

Anderson, Benedict. 1991. *Imagined Communities: Reflections on the Origins and Spread of Nationalism*. Verso: New York.

An Introduction to E-Tagging. 2002. T-15-0102, Gartner Inc., January 11.

Baker, Chris. 2003. "Channel 7 uses GPS to dispatch its crews: Some workers see privacy violation." *The Washington Times*. P C11. January 23, Available: www.global.factiva.com

Bell, Daniel. 1971. *The coming of post-industrial society: A venture in social forecasting,* Basic Books: New York.

Bennett, Colin, Raab, Charles and Regan, Priscilla. 2003. "Patterns of individual identification within intelligent transportation systems", In David Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Routledge: New York, pp.153-175.

Blackwell, Gerry. 2001. "Location, location, location." *Wireless Telecom,* Vol. 19, No. 3. pp. 38-46.

Brave Mobile World: Emerging Technologies for Mobility. 2001. T-14-0297, Gartner Inc. October 1.

Castells, Manuel. 2004. *The Power of Identity*. Blackwell: Oxford.

Cavoukian, Ann. "Privacy Protection is Good Business" Speeches 2000-2005, Available: www.ipc.on.ca/speeches/.

Charny, Ben. 2004. "Big Brother Likely to Be Big Boss." *The Atlanta Journal*. P A1. , September 24, Available: www.global.factiva.com

Cho, Dan. 2004. "Space Tracker." *Technology Review*, December.

Church, Jack. 2004. "Keeping tabs on teens, by cellphone", *Ottawa Citizen*, September 22, A3.

Connolly, Allison. 2005. "Securing your networks against the risk of rogue wireless access is no longer optional". *ComputerWeekly.com*. January 25. Available: http://www.computerweekly.com.

Cribb, Robert. 2005. "Car Tracking: Useful tool also gives you the creeps", *The Toronto Star*, March 21, Available: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&call-pageid=971358637177&c=Article&cid=1111359009544.

Crowe, David. 2004. "Wi-Fi, Wi-Max: Taking wireless security seriously", *Wireless Telecom*, Issue 3, pp. 36-39.

Curry, Michael R., Phillips, David J. and Regan, Priscilla M. 2004. "Emergency Response Systems and the Creeping Legibility of People and Places". *The Information Society*, Vol. 20, pp. 357-369.

Danna, Anthony & Gandy, Oscar H. Jr. 2002. "All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining". *Journal of Business Ethics*, Vol. 40, pp. 373-386.

EKOS Research Associates Inc. 2003. *Canadians' Views Towards a National ID Card and Biometrics,* March 31.

Enterprises should care about U.S. E911 Evolution. 2002. COM-14-9382, Gartner Inc. January 22.

European Symposium Mobile Technology Survey. 2002. COM-14-9382, Gartner, Inc. January 22.

"'Evil Twin' threat to Wi-Fi users". 2005. *CNN.com*. January 20. Available: http://edition.cnn.com/2005/TECH/internet/01/20/evil.twins/index.html.

"eXI'S Shareholders vote in favour of proposed acquisition by Applied Digital's VeriChip", 2005, *CNW Group*, March 14, Available: www.canadanewswire.ca/en/releases/archive/March2005/14/c4589.html.

Gandy, Oscar H. Jr. 1996. "Coming to Terms with the Panoptic Sort". In *Computers, Surveillance & Privacy*. David Lyon & Elia Zureik (Eds.), University of Minnesota Press: Minneapolis.

Gartner's Glossary of Wireless Mobile Terms: 2002 Update. 2002. Strategic Analysis Report, Gartner Inc., June 12.

Gottlieb, Calvin C. 1996. "Privacy: A Concept Whose Time Has Come and Gone". In *Computers, Surveillance & Privacy*. David Lyon & Elia Zureik (Eds.), Minneapolis : University of Minnesota Press.

Gow, Gordon A. 2004a. *Prepaid Mobile Phone Service: the Anonymity Question*. Paper presented at the Canadian Communication Association Annual Conference, June 2004.

Gow, Gordon. 2004b. *Pinpointing Consent: Location Privacy and Mobile Phones*. Paper prepared for 'The Global and the Local in Mobile Communication' Conference. June 10-11, 2004.

Gratton, Eloise. 2002. "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising". *Canadian Journal of Law and Technology*. Vol. 1, No.2, November, pp. 59-78.

Green, Nicola and Smith, Sean. 2004a. *Regulation, Information and the Self: Ownership in Mobile Environments*. Intel Architecture Labs, Available: http://risome.soc.surrey.ac.uk/info.htm.

Green, Nicola and Smith, Sean. 2004b. "A Spy in your Pocket? The Regulation of Mobile Data in the UK." *Surveillance & Society*. Vol. 1, No. 4, pp. 573-587.

Hamilton, Tyler. 2005. "Telecoms feel heat on wiretaps", *Toronto Star*, January 22.

Harris, Marvin. 1978. *Cannibals and Kings: The Origins of Cultures*. Vintage Books: New York.

Harris, Shane. 2004. "Private Eye", *Govexec.com*, March 16, Available: http://www.govexec.com/features/0304/0304s1.htm.

Hilzik, Michael A. 2004. 'Woz goes Wireless', *Technology Review*, vol. 107, no. 4, May, pp. 42-45.

How Enterprises Use Wireless Devices for Real-Time Benefit. 2003. COM-19-4970, Gartner Inc., April 8.

"How Location Tracking will work", *Howstuffworks.com*, Retrieved: December 20, 2004, Available: http://people.howstuffworks.com/location-tracking.htm/printable.

"How Bluetooth Works." *Howstuffworks.com*, Retrieved: December 12, 2004, Available: http://electronics.howstuffworks.com/bluetooth.htm.

"How Ubiquitous Networking Will Work." *Howstuffworks.com*, Retrieved: December 12, 2004, Available: http://computer.howstuffworks.com/ubiquitous-network.htm.

Introna, Lucas D. 2003. "Workplace Surveillance 'is' Unethical and Unfair." *Surveillance & Society*. Vol. 1, No. 2. pp. 214.

Kumar, Sameer and Kevin Moore. 2002. "The Evolution of Global Positioning System Technology." *Journal of Science and Education Technology*. Vol. 11, No. 1. pp. 59-80.

"Law-enforcement agencies are learning the value of using GPS to keep a constant eye on some released prisoners", 2004. *The Feature*, July 12, Retrieved: February 12, 2005, Available: http://www.thefeature.com/article?articleid=100867.

Lemos, Robert. 2001. "State puts brakes on GPS speeding fines", *News.com*, July 2, Available: http://news.com.com/2100-1040-269388.html?legacy=cnet.

Location-Based Services and Telematics, 2002. COM-17-0277, Gartner Inc., July 16.

Lyon, David. 2005. "Why where you are matters: mundane mobilities, transparent technologies and digital discrimination," unpublished paper.

Lyon, David. 2004. *Surveillance after September 11*. Polity: Cambridge.

Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*, Polity: Cambridge.

"Make it Simple." 2004. *The Economist.com*, October 28, Retrieved: January 24, 2005, Available: www.economist.com/surveys/PrinterFriendly.drm?Story_ID+3307363.

Marx, Gary T. 2003. "A tack in the Shoe: Neutralizing and Resisting Surveillance". *Journal of Social Issues*. Vol. 59, No. 2. pp. 165-189.

Marx, Gary T. 1999. "Measuring Everything That Moves: The New Surveillance at Work". In I. Simpson & R. Simpson (Eds) *Research in the Sociology of Work*. Stamford: Jai Press Inc. pp. 165-189.

Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. University of California Press: Berkeley.

McCullagh, Declan. 2005. "Senator predicts 'overdue' changes to privacy". *News.Com*. March 10, Available: http://news.com/2102-1029_3-5608455.html.

McKeefry, Hailey Lynn. 2004. "Location-Based Services Come of Age", *Mobilized Software*, Retrieved: March 3, 2005, Available: www.mobilizedsoftware.com/showArticle.jhtml?articlesId=18901516.

Media Awareness Network, 2004. "'Young Canadians in a Wireless World' Phase Two Findings: Privacy, Intimacy, Security and Ethical Behaviour", Available: www.media-awareness.ca/english/special_initiatives/surveys/phas_two/upload/yccww_phase_two_report.pdf/.

Millard, Elizabeth. 2005. "ChoicePoint Discloses Massive Identity Theft." *CRM Daily*, February 17, Available: http://crm-aily.newsfactor.com/story.

Mobile and Wireless Services and Service Providers in Canada. 2004. DPRO-92579, Gartner Inc., July 9.

Mobile Location Services: No Mass Market in Europe Until 2007, 2001. Gartner Inc., July 9.

"Move Over, Big Brother." 2004. *The Economist.com,* December 2, Retrieved: January 24, 2005, Available: www.sysopt.com/PrinterFriendly.cfm?Story_ID=3422918.

Mowshowitz, Abbe and Zureik, Elia. 2004. *Consumer Power in the Digital Society*. University of Minnesota Press: Minneapolis.

Murphy, Shannon. 2004. "How to Choose a GPS Fleet Management System: What Features are Right for You?" *Management Quarterly*. Vol. 45, No. 2, July 1, pp. 30. Available: www.gobal.factiva.com.

Owen, Gareth and Peter Richardson. 2001. *Mobile Location Services: No Mass Market in Europe Until 2007*. M-17-7758, Gartner, Inc. September 5.

Patten, Brad. 2004. "Pay attention to your security with wireless networks" *The Business Journal of Jacksonville*, November 29.

Pfeiffer, Eric W. 2005. "WhereWare", *Technology Review*, Retrieved: January 26, 2005, Available: www.technologyreview.com/articles/03/09/pfeiffer0903.asp?p=0.

Phillips, David & Curry, Michael. 2003. "Geodemographics and the changing spatiality of local practice." In *Surveillance as Social Sorting*. David Lyon (Ed.). Routledge: New York.

"Portable Pathfinder." 2004. *Technology Review*, October.

Prasad, Maneesh. "Location Based Services." *GIS Development*, Retrieved: January 21, 2005, Available: www.gisdevelopment.net/technology.lbs.techlbs003pf.htm.

"Privacy: Commercial MLS launches are delayed by fears of 'Big Brother'". 2003. *Mobile Location Analyst*. October, pp. 3-35.

Privacy Commissioner of Canada, 2000. *The Personal Information Protection and Electronic Documents Act*, Available: http://www.privcom.gc.ca/legislation/02_06_01_e.asp.

Raddcomm Wireless Consulting Services L.L.C. "Location Methods for E-911 Phase II", Available: http://www.raddcomm.com/E-911%20Location%20Methods.htm.

Rogal-Black, Mary. 2004. "Hotspots here, there and everywhere." *Backbone Magazine*. November/December, pp. 20-22.

Schneier, Bruce. 2005. *Schneier on Security*. February 14, Available: http://www.schneier.com/blog/archives/2005/02/tmobile_hack.html.

Schneier, Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World*, Wiley Computer Publishing: New York.

Slater, Don. 1997. *Consumer Culture and Modernity*. Polity: Cambridge.

Smart Cards, Smart IDs and the Semiconductor Industry. 2003. Gartner Inc., Research Brief, July 28.

"Software Defined Radio (SDR)." 2005. *OWRA/IEEE COMSOC/NCIT/CRC Seminar Day*, January 14, Ottawa.

"Something to watch over you." 2002. *Economist.com,* March 13, Retrieved: January 24, 2005, Available: www.economist.com/PrinterFriendly.cfm?Story_ID=1280634.

Stalder, Felix. 2002. "Privacy is not the antidote to surveillance." *Surveillance & Society,* Vol. 1 No. 1, pp. 120-124. Available: http://www.surveillance-and-society.org/articles1/opinion.pdf.

"Study: 'Texting on the Rise'". 2005. *Associated Press*, March 17.

Surtees, Lawrence. "Nowhere to Hide: Privacy Implications of Wireless Location Technology", *IDC Canada*, #CA025TLH, Vol. 1.

"Telus partners with ViaVis Mobile Solutions to trial voice-activated, location-based Web service", 2005. News Releases, *Telus Media*, Retrieved: March 14, 2005, Available: http://about.telus.com/cgi-bin/news_viewer.cgi?mode=2&news_id=291.

Tracking People, Products and Assets in Real Time. 2003. COM-19-7533, Gartner Inc., April 18.

Tristram, Claire. 1999. "Has GPS lost its way?" *Technology Review*, July/August, Retrieved: February 7, 2005, Available: http://www.technologyreview.com/articles/99/07/tristram0799.asp?p=1.

"The Wireless Wreck", 2004. *Technology Review*, September.

"The revenge of geography." 2003. *The Economist.com*, March 13, Retrieved: January 24, 2005, Available: www.economist.com/PrinterFriendly.cfm?Story_ID=1620794.

User location data will give MNOs an edge. 2001. TG-14-0934, Gartner Inc. July 17.

"What is a hot-spot." *Webopedia*, Retrieved: March 10, 2005, Available: http://www.webopedia.com/TERM/G/GPS.html.

"What is GPS?" *Webopedia*, Retrieved: January 1, 2005, Available: http://www.webopedia.com/TERM/G/GPS.html.

White, James C. 2003. "People, Not Places: A Policy Framework for Analyzing Location Privacy Issues." Masters Memo Prepared for the Electronic Privacy Information Center, Duke University, Spring, Retrieved: January 12, 2005, Available: http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf.

Winseck, Dwayne. 2001. "Netscapes of Power: Convergence, Network Design, Walled Gardens and Other Strategies of Control in the in the Information Age". In, David Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. Routledge: New York, pp. 176-198.

"Wireless City showcases Calgary tech", 2004. *Backspace Magazine*, Nov/Dec, pp. 18.

"Wireless Fact and Figures", 2004. *Industry Facts*, CWTA, Retrieved: December 20, 2004, Available: www.cwta.ca/CWTASite/english/industryfacts.html.

Wireless Location Services for Telematics have yet to Thrive, 2002. Technology Analysis, Gartner Inc., July 23.

"Wireless on Wheels", 2002. *Technology Review*, Jan/Feb.

Wood, Anne Marie. 1998. "Omniscient Organizations and Bodily Observations: Electronic Surveillance in the Workplace." *International Journal of Sociology and Social Policy*. Vol. 18, No. 5/6. pp. 132-169.

Zeller, Tom Jr. 2005. "Breach Points Up Flaws in Privacy Laws". *The New York Times*, February 24, Available: http://www.nytimes.com/2005/02/24/business/24datas.html.

Zureik, Elia. 2004. *Appendix A: Overview of Public Opinion Research Regarding Privacy*. Globalization of Personal Data Project, International Survey Concept Paper, March 3, Available: http://www.queensu.ca/sociology/Surveillance/Overview%20Appendix%20A.pdf.

Zureik, Elia. 2003. "Theorizing Surveillance: The Case of the Workplace", in David Lyon (Ed) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination,* New York: Routledge, pp. 31-56.