M-Commerce in Canada: An Interaction Framework for Wireless Privacy

Constantinos Coursaris, Khaled Hassanein, Milena Head
McMaster University

Abstract
Mobile commerce (m-commerce) is a natural extension of e-commerce that allows users to interact with other users or businesses in a wireless mode, anytime/anywhere. The Canadian market, with its high rates of technology acceptance, should be a fertile ground for m-commerce growth. This paper will examine m-commerce in the Canadian landscape, focusing on wireless privacy issues. We start with an introduction of m-commerce and an examination of its similarities and differences with e-commerce. An overview is presented of the Canadian landscape for both e-commerce and m-commerce, followed by a discussion of the needs and concerns of the mobile consumer (m-consumer). We then examine privacy issues associated with e-commerce and identify additional privacy concerns that arise due to the wireless nature of the m-commerce environment. Consequently, a new wireless privacy interaction framework is introduced which reflects the nature of interactions taking place between parties within a wireless environment. The responsibilities of the interaction parties towards enhancing the privacy of the m-consumer are then outlined. The paper ends with some conclusions and potential directions for future research.

Résumé
Le commerce mobile (commerce-m) est une excroissance naturelle du commerce électronique qui permet, en tout et en tous lieux, la communication sans fil entre ses utilisateurs. Le marché canadien, marqué par des taux élevés d'intégration technologique, est un terrain de prédilection pour le développement de ce nouveau type de commerce. Le présent article, qui met l'accent sur les questions de confidentialité liées à la communication sans fil, analyse la situation du commerce mobile au Canada. Nous commençons notre étude par une définition du concept de commerce mobile et un examen des points de ressemblances et de différences entre celui-ci et le commerce électronique. Ensuite, nous proposons un aperçu général du commerce électronique et du commerce mobile dans le paysage canadien, suivi d'une analyse des besoins et des soucis des consommateurs du commerce électronique (consommateurs mobiles). Plus loin nous examinons les problèmes de confidentialité liés au commerce électronique, et les problèmes supplémentaires générés par le caractère sans fil du commerce mobile. C'est pourquoi nous introduisons un nouveau cadre d'interaction de la confidentialité sans fil, cadre qui reflète la nature des interactions qui existent entre les parties dans un environnement pareil. À ce niveau, nous insistons sur les responsabilités des parties prenantes dans le renforcement de la confidentialité du commerce mobile. Nous achevons notre étude par quelques conclusions et des propositions de pistes potentielles de recherches futures.

From its inception and over the last two decades, the Internet has undergone significant change. Although the Internet was designed before local area networks (LANs) existed, it has adapted to suit new network technologies, such as client-server and peer-to-peer computing, and telecommunication services, such as asynchronous transfer mode (ATM) and frame-switched services. Consequently, the ability to engage in transactions for either personal or professional use over the Internet has emerged and is known as electronic commerce or e-commerce. The most recent trend of e-commerce involves expanding the services offered and extending the reach to customers through powerful, affordable computing and communications in portable form, that is, laptop computers, two-way pagers, personal digital assistants (PDAs), and cellular phones. The mobility associated

Address correspondence to Khaled Hassanein, Michael G. DeGroote School of Business, McMaster University, 1280 Main Street West, Hamilton, ON, Canada L8S 4M4. E-mail: hassank@mcmaster.ca

with these devices has resulted in naming this new trend mobile commerce or m-commerce (Leiner et al., 2002).

M-commerce utilizes wireless networks to enable users to transmit data between mobile and other computing devices using wireless adapters without requiring a wired connection. The recent hype surrounding wireless networks revolves around the third-generation (3G) systems, expected to be deployed over the next few years, with certain regions (e.g. Japan) already having access to them. These networks are commonly referred to as IMT-2000 on a global scale, and regional implementations are uniquely named, for example, CDMA2000 (for Code-Division Multiple Access) in North America, wideband CDMA (W-CDMA) or Universal Mobile Telephony System (UMTS) in Europe and Japan, and cdmaOne in Japan. Along with voice functionality, 3G networks support higher-speed transmissions for high-quality audio and video, as well as providing a global "always on" roaming capability (Peck, 2001). Until recently, wireless devices could be classified in three distinct categories: mobile phones, wireless PDAs, and wireless laptops. Recently, however, hybrid products have been introduced that combine features from two or all three categories with the intent of providing optimal capabilities to mobile users. The most recent development in mobile devices was the introduction of "smart phones". These are mobile devices capable of tasks ranging from e-mail retrieval, available now, to video and music streaming in the near future. Smart phones are a combination of cell phones and PDAs (e.g. Kyocera QCP™ 6035 Smart Phone, Samsung SPH-I300) (Pocket Directory, 2001). This convergence trend is expected to continue in the foreseeable future to support consumer demands for mobile devices that can provide a wider range of capabilities (Keyte, 2001).

Canada has maintained a rapid pace in terms of adapting new technologies. In 1997, the World Economic Forum ranked Canada first among the G7 in terms of technology potential, and according to the Organisation for Economic Co-operation and Development, Canada was first among the G7 in home computer, cable, and telephone penetration for the same year. Canadian eagerness for adoption of new technologies was reinforced the following year (October 1998), when the World Information Technology and Services Alliance released a study ranking the 50 largest economies based on expenditure on hardware, software, technology services, telecommunications, and office equipment. Canada ranked third on a per capita basis, behind the United States and Japan, in technology spending for the previous year. Furthermore, Canadians showcase high penetration rates for Internet and mobile phone usage (Manley, 1998).

This paper starts with a review of the similarities and differences between m-commerce and e-commerce, followed by an overview of the Canadian landscape for both e-commerce and m-commerce. The second section continues with a discussion of the needs and concerns of the m-consumer (mobile consumer) and an overview of m-commerce business applications, identifying privacy and security as key concerns. The third section explores privacy issues associated with e-commerce and identifies additional privacy concerns that arise due to the wireless nature of the m-commerce environment. In the fourth section, we introduce a wireless privacy interaction framework, which reflects the nature of interactions within a wireless setting. The responsibilities of the interaction parties towards enhancing the privacy of the m-consumer are then outlined through a wireless privacy party-to-party responsibilities matrix. The fifth section discusses the wireless privacy implications to the parties identified within the wireless privacy interaction framework. The final section provides some conclusions and potential directions for future research.

M-Commerce Overview

The name m-commerce arises from the mobile nature of the wireless environment that supports mobile electronic transactions. Devices, including digital cellular phones, PDAs, pagers, notebooks, and even automobiles, can already access the Internet wirelessly and utilize its various capabilities, such as e-mail and Web browsing (Little, 2001). M-commerce is a natural extension of e-commerce as they share fundamental business principles, but m-commerce acts as another channel through which value can be added to e-commerce processes. It also provides for new potential ways to meet evolving customer needs.

Similarities and Differences

The m-commerce and e-commerce business environments and activities have a lot in common since they involve much of the same functionality in terms of facilitating electronic commerce over the Internet. However, some differences exist in the mode of communication, the types of Internet access devices, the development languages and communication protocols, and the enabling technologies used to support each environment. Differences in these four areas are explored below in more detail (Little, 2001).

Communication mode. The main mode of conducting wired e-commerce is through a wired connection to a LAN while for m-commerce it is through a wireless network. This is a fundamental difference between the two environments as it enables customers to engage in m-commerce anytime/anywhere using various forms of wireless communication devices (e.g. cell phones or PDAs).

Internet access devices. Wired e-commerce is conducted mainly through desktop and laptop computers. M-commerce, on the other hand, is conducted through a variety of wireless devices including cell phones, PDAs, and wireless-enabled laptops. Since most of these devices are more personal in nature than the usual desktop (i.e. they tend to be used by a single user who carries the device at most times), the potential for offering personalized products and services is higher. This trend is further enhanced by the ability of some wireless devices to implicitly convey the current whereabouts of their user, which makes it possible to make location-aware offers to mobile consumers. This also gives rise to more prominent privacy concerns than those experienced by consumers of wired e-commerce.

Development languages and communication protocols. Most people are familiar with the hypertext markup language (HTML), the language that runs the wired Web. Mobile devices, however, are running on one of two variations of HTML: wireless markup language (WML) or compact HTML (cHTML). WML is used in most parts of the world, whereas cHTML is used by DoCoMo in Japan with plans for expansion. The need for WML and cHTML is due to mobile devices having to comply with new communication protocols, such as the wireless application protocol (WAP) and DoCoMo's (Japan) proprietary protocol i-Mode. Different from the wired Web's hypertext transfer protocol (HTTP), these new protocols present issues of compatibility and functional limitation.

Enabling technologies. Functional limitations arise in the m-commerce environment as many of the existing technologies that enable e-commerce on the Web with relative ease (e.g. cookies, JAVA, active server pages, etc.) are not compatible with WAP, for example. Although new standards that would address these issues (i.e. WAP 2.0) are currently under development, a tested and trustworthy system is still absent.

M-Commerce in Canada

Fulfillment of market interest in e-commerce requires establishing a wired infrastructure necessary to enable electronic transactions. As interest in e-commerce grows, so does the need for additional infrastructure. Since m-commerce acts as a new channel for e-commerce, it will be able to leverage the existing infrastructure. Hence, growth in e-commerce supports further growth in m-commerce. To predict the potential for m-commerce then, it would be useful to examine the growth in e-commerce. Some metrics that illustrate the growth potential for e-commerce include the following (Statistics Canada, 2001):

Internet penetration rates (Figure 1). There was an increase in regional Internet penetration rates across Canada, bringing the national generation level to over 50%. Overall, there was a 25% growth rate in Internet use from all locations.

Internet use frequency. In 2000, 71% of Canadian households had at least one person who regularly used the Internet from home a minimum of seven times a week, up from 65% in 1999 (a growth rate of 9%). In addition, in 2000, 61% of Canadian households had someone who spent 20 hours or more a month on the Internet, up from 47% in 1999 (a growth rate of 30%).

E-commerce level. 12% of Canadian households placed at least one order over the Internet from home, regardless of whether or not they paid on-line (a growth rate of 81% since 1999). The subset of these households that actually made an on-line payment for at least one of their transactions experienced an even higher growth rate of 88% to reach a total of 10% of Canadian households. Furthermore, there was a growth of 46% in 2000 to reach a level of 22% of all Canadian households that used the Internet to shop, without necessarily purchasing on-line (i.e., researched and proceeded with purchase offline). The average expenditure per on-line order was $121.

Internet applications (Figure 2). Most households access the Internet from home for e-mail and Web browsing. Other popular reasons for going on-line include searching for medical and health-related information (57%), e-banking (37%), and to find employment (31%).

Comparing the Canadian e-commerce market with the rest of the world reveals that Canadians were among the world's top Internet users in 2000. Leading the pack, 73% of Canadians and Swedes were on-line last year, edging the U.S., which had 72%. It now appears that the United States is leveling off in terms of Internet use growth, whereas Canada and Europe continue to grow, perhaps in part due to a more even distribution of income and more concentrated population centres (Ipsos-Reid, 2001). Furthermore, in the Canadian business landscape e-commerce is also becoming an integral part of a company's infrastructure. There was a growth of 73% for the value of orders received by the private sector over the Internet (with or without on-line payment) to reach a total $7 billion, translating to a two-fold increase in total operating revenue from 0.2% to 0.4% (Statistics Canada, 2001). In 2000, approximately one in five private enterprises bought goods or services over the Internet. Nearly all public sector institutions used the Internet in 2000, while approximately three in four public institutions had a Website (Statistics Canada, 2001). These statistics show that Canadian consumers are receptive to the new

Figure 1
Canadian Internet Penetration Rates by Province (Statistics Canada, 2001)

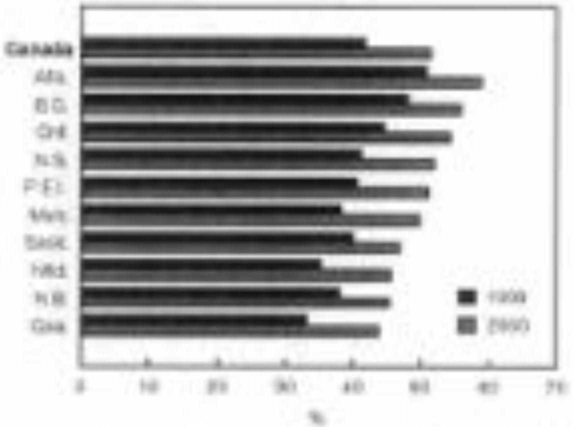
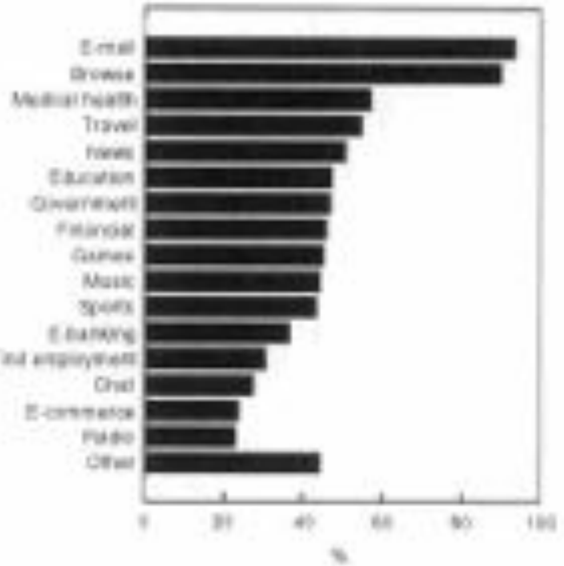


Table 1
Comparing Canada and U.S. Adoption Rates for Various Technologies

Technology	U.S. (Figure 3)	Canada
Mobile Internet	25%	24% (CWTA, 2002)
PC Internet	26%	50% (StatsCan, 2001)
Cell Phone	24.4%	29% (CWTA, 2002)
PC	40%	61% (ACNielsen, 2000)
Telephone	93.9%	96% (StatsCan, 2001)

Figure 2
Internet Applications Frequently Accessed by Regular Canadian Users from Home, 2000 (Statistics Canada, 2001)



on-line medium, and Canadian businesses are willing to explore and invest in these technologies.

Figure 3 shows how the relative adoption rate of wireless Internet services in the U.S. exceeds that of previous major technologies (Morrison, 2001), including e-commerce enabled through PC Internet adoption. Table 1 suggests that Canada matches closely or outperforms the U.S. in penetration rates of all the technologies described in Figure 3. Thus, we expect the Canadian market to exhibit a similar trend for wireless Internet to that shown in Figure 3 for the U.S. Furthermore, according to some forecasts, the global customer base for wireless Internet access is expected to match the overall wireless subscriber base by 2004 (Morrison, 2001).

The Canadian m-commerce market is young but evolving quickly. With investments exceeding $8 billion since 1995 in mobile phone communication infrastructure and $1 billion since 1996 in wireless infrastructure in Canada every year, the wireless industry in Canada generated revenues of $5.5 billion in 2000 (see Figure 4), a growth of 20% since 1999 (Canadian Wireless Telecommunications Association, 2002). Factors affecting this growth include (a) new government regulatory policies (e.g. local number portability) that may help minimize the impact of artificial barriers currently limiting transition from wired to wireless; (b) increasing affordability of wireless relative to wired usage; and (c) increasing availability of services and products addressing consumer needs.

The largest component of the Canadian m-commerce market comes from the wireless phone industry, which has experienced a tremendous growth since its inception in 1985. In particular, during the last five years there were approximately 30% new wireless phone subscribers each year, making wireless phones one of the fastest growing consumer products in Canadian history.

Revenue from voice service is typically included in the financial analysis for m-commerce because it is earned by wireless network operators, who are also responsible for supporting data services. Voice revenue is then used to support the wireless industry and promote growth for both voice and data services. Overall, there are approximately 12 million wireless devices currently used by Canadians on a daily basis, including 9 million wireless phones (see Figure 5), more than 1.8 million pagers, 1 million mobile radios, and 10,000 mobile satel-

Figure 3
U.S. Adoption Rates for Various Communication and Internet Access Devices (Morrison, 2001)

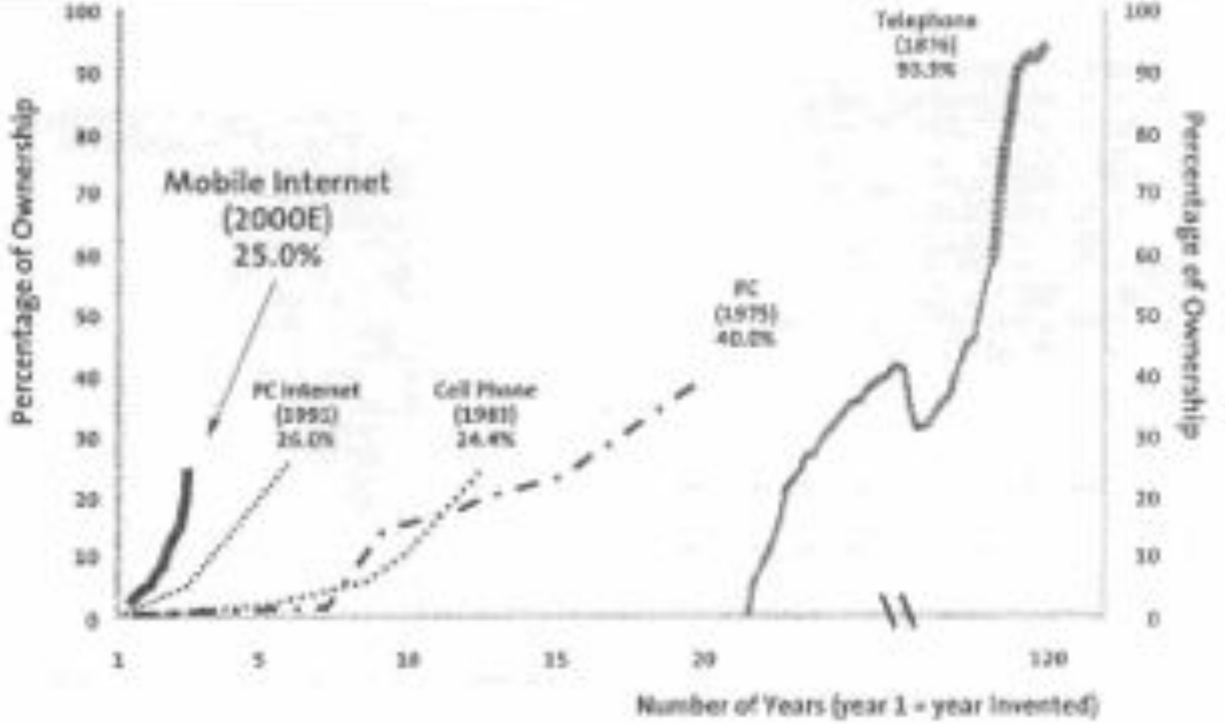


Figure 4
Canadian Cellular/PCS Revenue in $ Billions (CWTA, 2002)

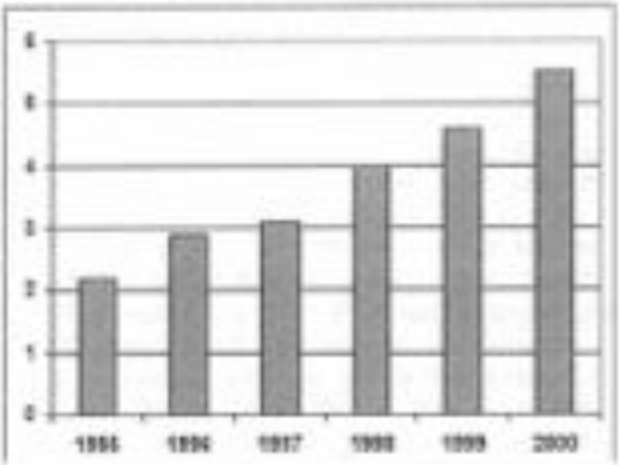
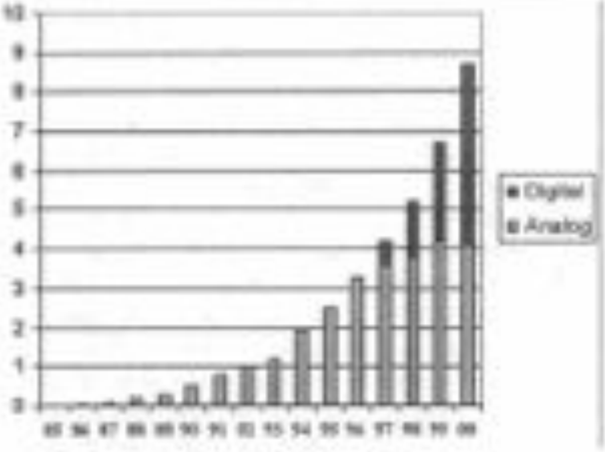
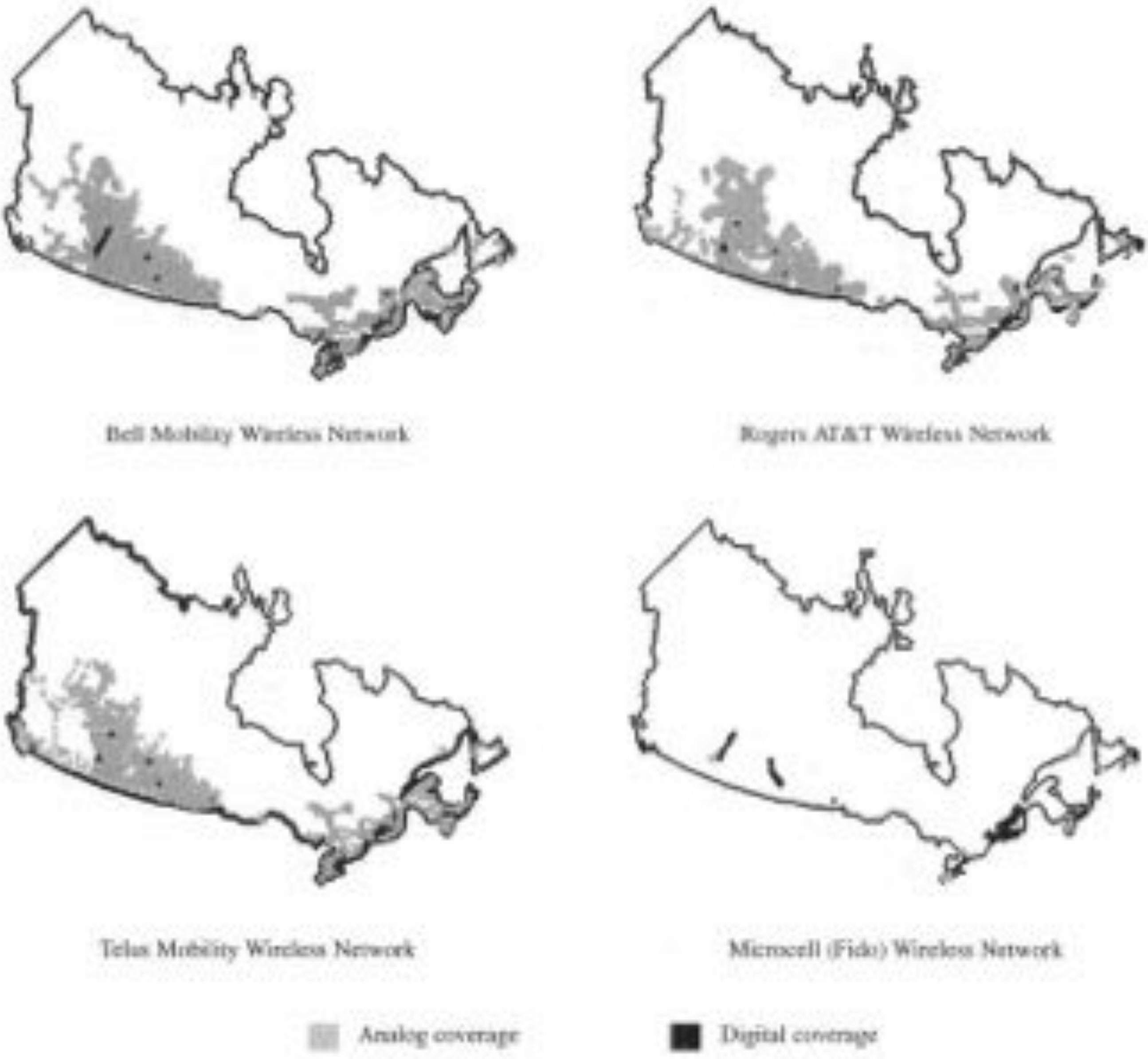


Figure 5
Canadian Cellular/PCS Growth in Millions of Subscribers (CWTA, 2002)



line phones. Thus, almost one in every four Canadians has access to a wireless device in one form or another. Canadians use their mobile phones for 185 minutes per month on average, and 4% of all Canadians are already using wireless Internet service with 24% expected to subscribe to this service next year. These numbers,

Figure 6
Wireless Networks in Canada



Bell Mobility Wireless Network

Rogers AT&T Wireless Network

Telus Mobility Wireless Network

Microcell (Fido) Wireless Network

although promising, are still behind a number of countries, including four that showcase mobile penetration rates exceeding 70%: Finland (75%), Hong Kong, United Kingdom, and Norway (74%) (Accenture, 2001).

More than half of all Canadians have a choice of four wireless communications providers: Bell Mobility (3,919,450 subscribers), Microcell Connexions (1,209,210 subscribers), Rogers AT&T Wireless (2,991,900 subscribers), and TELUS Mobility (2,570,000 subscribers) (CWTA, 2002). Network coverage is critical in generating new subscriptions. Figure 6 shows wireless network coverage maps for each of the four major carriers. The shaded areas in these maps represent analog wireless coverage, whereas the dark areas represent digital wireless coverage.

Based on the maps shown in Figure 6, it is clear that the vast majority of Canadians (93%) have access to analog wireless services, since most live in the southern parts of Canada. Additionally, a large proportion of Canadians (85%) also have access to digital wireless services, which centre on the highly populous metropolitan areas (Rogers Communications, 2002). Hence, with the infrastructure in place, content development combined with appealing marketing campaigns should drive wireless penetration rates even higher. In addition, the presence of four wireless network carriers increases the likelihood of improved quality of service, a consequence of pressure exerted by competition.

M-Consumer Needs and Concerns

Five primary needs can be identified that yield demand for m-commerce services. These five needs stem from the mobility associated with the enabling devices, so the context for each of them revolves around the theme of "anytime, anywhere" accessibility (Coursaris & Hassanein, 2002).

Connectivity needs. Connectivity provides the basic platform on which wireless communications take place. In a ubiquitous wireless environment that overcomes geographic (i.e., location of the consumer) and compatibility (i.e., interoperability of networks) constraints, consumers become capable of true anytime, anywhere communication.

Communication needs. Communication with others for either business or personal purposes (i.e. with other consumers or personal networks) may be carried out in an information, entertainment, or commerce context.

Information needs. M-consumers need access to static or dynamic information. Examples for these two categories would include a yellow pages-type directory (static) and cross-referencing of wireless Websites for prices or specifications of a particular product (dynamic). In addition, mobile users need access to location-specific information (e.g. finding a nearby restaurant based on the user's search criteria and current location).

Entertainment needs. Users want to turn to their mobile devices to get useful and practical entertainment solutions, such as access to games or leisure information.

Commerce needs. Two main elements are required to enable mobile consumers to conduct m-commerce transactions: presentation of product/service information and a wireless payment mechanism. The value in consumers making payments wirelessly arises from the convenience it offers. For example, mobile users might not require coins/bills to make certain physical purchases (e.g. from vending machines), digital purchases (e.g. purchases on a wireless Website), or even bill payments (e.g. mobile bill presentment and payment).

A wide range of consumer concerns arise in the m-commerce environment. The main concerns are summarized below (Coursaris & Hassanein, 2002).

Privacy. In the information context, privacy refers to a user's fear of other people/organizations knowing what he or she is interested in ("Big Brother syndrome"). Tracking user Internet-browsing behaviour and information requests on the wireless Web is a sensitive topic, as it is for its wired counterpart. The ability to know the exact location of a user at all times further escalates the sensitivity of the Big Brother syndrome. Another type of privacy concern for consumers in this area is that their location might be revealed to interested businesses at all times. Knowing the whereabouts of each mobile user may be perceived as threatening to the m-consumer, as this information could be dangerous if intercepted.

Security. Consumer fears regarding the safety of the information exchanged over a wireless network increases with the degree of interaction and the sensitivity of the information exchanged. Security is a critical component in protecting consumer privacy.

Reliability. For any extent of network coverage, it is important that the connection quality be maintained. The inherent concern here is that loss of the connection can result in loss of data (Nielsen, 2000).

Download times. Mobile users should not be forced to spend excessive amounts of time to access desired content (Cole, 2001).

Cost. Users of wired Internet access have the option of subscribing to different transfer rates, which come at different cost levels, subject to their individual needs. Aside from the cost of connecting to the wireless Web, there is also a pricing concern for the accessed information.

Usability. Information on the wireless Web should suit not only people's needs, but also the medium and the environment. For instance, content needs to be re-purposed for mobile devices so that users can access easy-to-digest pieces of news rather than long, replicated articles from the wired Web (McGinity, 2000). This notion ties in with usability, which raises questions about how easy it is for the mobile user to access the information sought and what the quality of the overall experience is. Factors influencing the quality of the overall experience include a user's ability to read the screen, input data, manipulate files, and access sites of interest.

In addition to the aforementioned concerns, limited content availability is a consideration that prevents customers from accessing the Internet wirelessly. Further frustration is experienced by users when they are victims of "walled gardens" (i.e., when they cannot access desired content because it is available only to users of other network carriers). Thus, accessibility and availability of content can serve as incentives not only for converting consumers to wireless Internet users, but also retaining these mobile users for the long run.

Canadian studies on ranking the above consumer

Table 2
Characteristics of M-commerce Consumer Business Applications

(Adapted from Coursaris & Hassanein, 2002)

	Need[1]					
Business Application	1	2	3	4	Interaction Modes[2]	Concerns
Communication						
- Voice	✓	✓	✓	✓	W_{B2C} W_{C2C}	Cost, Privacy
- SMS	✓	✓	✓	✓	W_{B2C} W_{C2C}	Cost
- E-mail	✓	✓	✓	✓	W_{B2C} W_{C2C}	Cost
- Data Transfer	✓	✓	✓	✓	W_{B2C} W_{C2C} W_C[3]	Cost
Information						
- Web browsing	✓	✓	✓	✓	W_{B2C}	Cost, Usability
- Traffic/Weather		✓			W_{B2C}	Privacy, Usability
Entertainment						
- Gaming			✓	✓		Cost, Usability
- News/Sports		✓	✓	✓	W_{B2C} W_{C2C}	Cost, Usability, Privacy, Download times, Cost
- Downloading Music/Video/Img.			✓	✓	W_{B2C}	Cost, Privacy
- Horoscope/ Lottery		✓	✓	✓	W_{B2C}	
Commerce						
- Ticketing (e.g. event, cinema)		✓		✓	W_{B2C}	Cost, Usability, Security, Privacy
- Pre-payment				✓	W_{B2C}	Security
- Banking		✓		✓	W_{B2C}	Security, Privacy
- Advertising		✓		✓	W_{B2C}	Privacy (Spam)
- Retailing		✓		✓	W_{B2C}	Security, Privacy, Usability

[1] 1. Communication, 2. Information, 3. Entertainment, 4. Commerce

[2] W_{B2C}: Wireless Business to Consumer Interaction, W_{C2C}: Wireless Consumer to Consumer Interaction, W_C[3]: Wireless Consumer to Self Interaction (e.g. with personal home network)

m-commerce concerns are not available yet; however, a recent study on e-commerce concerns identified privacy and security as the top two concerns for consumers (Head & Hassanein, in press). These concerns are expected to have an increased impact on m-commerce given the complexity and additional risks inherent in wireless transactions. The next section will present an overview of m-commerce business applications available in Canada and around the world and cross-reference them with the above concerns.

M-Commerce Business Applications

Various business applications targeting the mobile consumer are identified and presented in Table 2. In general, applications have been grouped under a need area in the first column of Table 2, based on the need to which they predominantly cater. The characteristics identified for each business application in Table 2 include the following (Coursaris & Hassanein, 2002): (a) consumer needs addressed by the business application; (b) wireless interaction modes covered by the business application; and (c) concerns associated with the business application.

The applications presented in Table 2 are those of highest interest to consumers and they often address multiple needs. For example, mobile banking would include options to access a user's account to obtain a balance, transfer funds, and even proceed with trading securities. This application, therefore, satisfies both the need to access information and the need to engage in commercial transactions.

What is of particular interest here is the overlap that exists between the identified wireless applications of interest to m-consumers and the most popular applications for the wired Internet Canadian users as indicated in Figure 2. Most of the applications between the two media (wired and wireless) match, except for Education, Government, Find Employment, and Medical Health. All other remaining categories, with interest exceeding 20% for each application on the wired Web, lend themselves well to the wireless medium. Although interest distribution may be different on the wireless Web, content availability in these areas could further promote growth of m-commerce. Currently, the following services are available in Canada: (a) communication, including voice, e-mail, chat, text messaging, data; (b) information, including 411, yellow pages, directions, updates (traffic and weather), travel deals, hotels, restaurants, taxi service, news (portals, business), agenda, address book; (c) entertainment, including games, listings (movies, event, sports), horoscope, lottery, ring tones; and (d) commerce, including bill payment, stocks (trading, quotes), bank account balance, purchase of goods.

The above services are available on digital networks (i.e. 2G and newer technologies). Future applications will be driven by the high bandwidth and associated high-speed rates of 3G technology. These applications will be targeting both consumers and businesses. For consumers, the focus of applications developed may be on consumer identification, since a mobile phone is a device that is most frequently associated with only one user. As such, the following examples of applications may be feasible: (a) storing credit card or bank account information on a mobile phone and using it to purchase; (b) storing full-colour photographs on a mobile device; (c) tracking or identifying the location of a mobile user; (d) videoconferencing using video and audio real-time feed to facilitate enhanced communication; (e) notifying with instant alerts (e.g. flight delay/cancellation); (f) finding nearest locations, lowest prices, and running promotions of merchants and their products/services.

With the introduction of the above applications, many consumer issues arise. Privacy is at the centre of attention, as control over personal information becomes even more challenging over wireless networks and presents a barrier for the success of m-commerce and related products and services. Hence, in the remaining part of this paper we focus our attention on the topic of wireless privacy.

Privacy Issues

Information privacy is the claim of individuals, groups, or institutions to determine for themselves when, and to what extent information about them is used and/or communicated to others (Agranoff, 1993). As mentioned, privacy and security are always among the top concerns for consumers. Often the two concepts are bundled together because of the less-than-clear distinction between them; however, privacy and security are distinct, albeit related, issues. Privacy requires security because without the ability to control access and distribution of information, privacy cannot be protected. However, security is not privacy. Information is secure if the owner of information can control that information, while information is private if the subject of information can control that information (Head & Yuan, 2001). Anonymous information has no subject, and thus ensures that information is private. Anonymity requires security and guarantees privacy, but is neither (Camp, 1999).

Privacy in E-Commerce

Consumer privacy concerns can be major inhibitors of e-commerce success. These concerns revolve around several on-line privacy principles or notions that are outlined below (NCR Corporation, 2003):

Purpose specification. At the time of collection of personal data, consumers should be provided with easily understood notice of the data collector's purpose(s).

Collection limitations. Personal data collected should be limited to fulfilling only the specified purpose(s).

Use limitations. The use of personal data should be limited to the purpose(s) specified above.

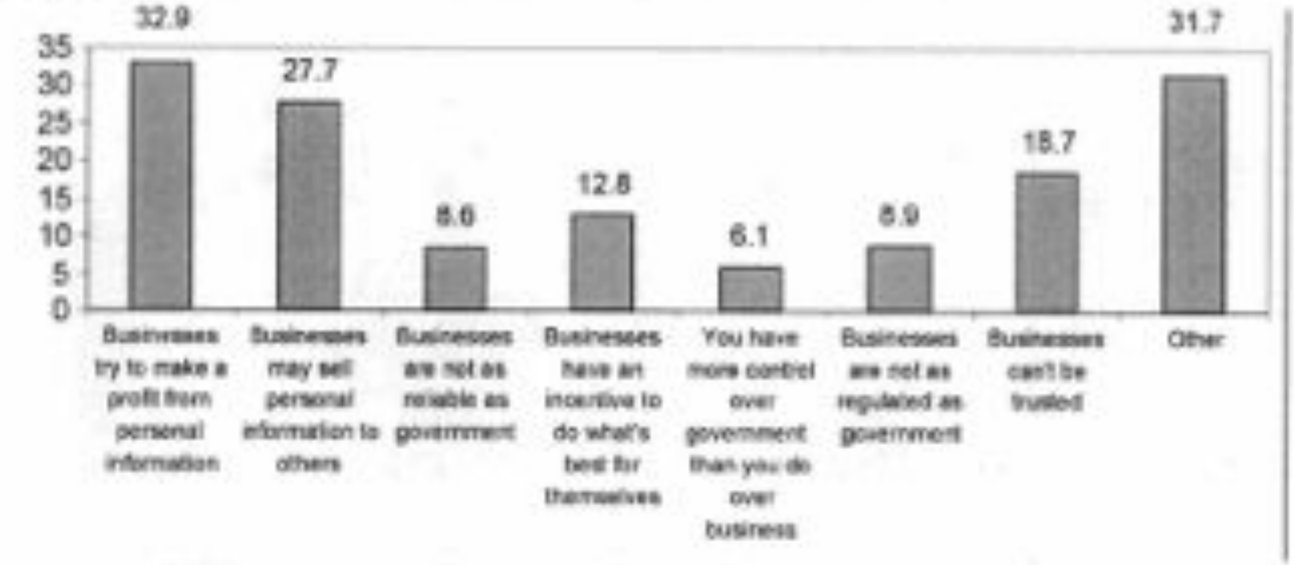
Time limitations. Data should not be kept in an identifiable form for longer than necessary to accomplish the original purpose(s).

Data quality. Personal data collected should be accurate, complete, and kept up-to-date.

Choice. Consumers should be offered suitable choices to opt-in or opt-out of specific personal data collection/use.

Access. Consumers should be provided the opportunity to examine any personal data kept about them and be able to rectify, amend, complete, or remove data where appropriate.

Figure 7
Reasons Cited for Privacy Concerns in Dealing with Businesses On-line (UCLA Center for Communication Policy, 2001)



Security. Personal data must be protected against possible loss, unauthorized access, or tampering.

Several data collectors are motivated to deviate from the above principles in search of profit. In other cases, hackers may seek to extract or intercept private information for political or ideological reasons, personal or financial gains, or even for sheer entertainment. Several examples exist where both business and government have violated consumer privacy for financial gains (Koster, 1999). The State of Illinois collects $10 million annually from the sale of public records. The State of New York collects over $49 million by selling information on motorists. The U.S. Post Office sells its 108 million permanent change-of-address cards, filed by people who move, to direct marketers.

These types of illegal or unethical activities are impacting e-commerce. According to the UCLA Internet Report (UCLA Center for Communication Policy, 2001), 94.4% of respondents are concerned about privacy, up 3.2% from 2000. It is interesting to note that there was an increase of 10% in respondents from the previous year who are either "very concerned" or "extremely concerned" about on-line privacy.

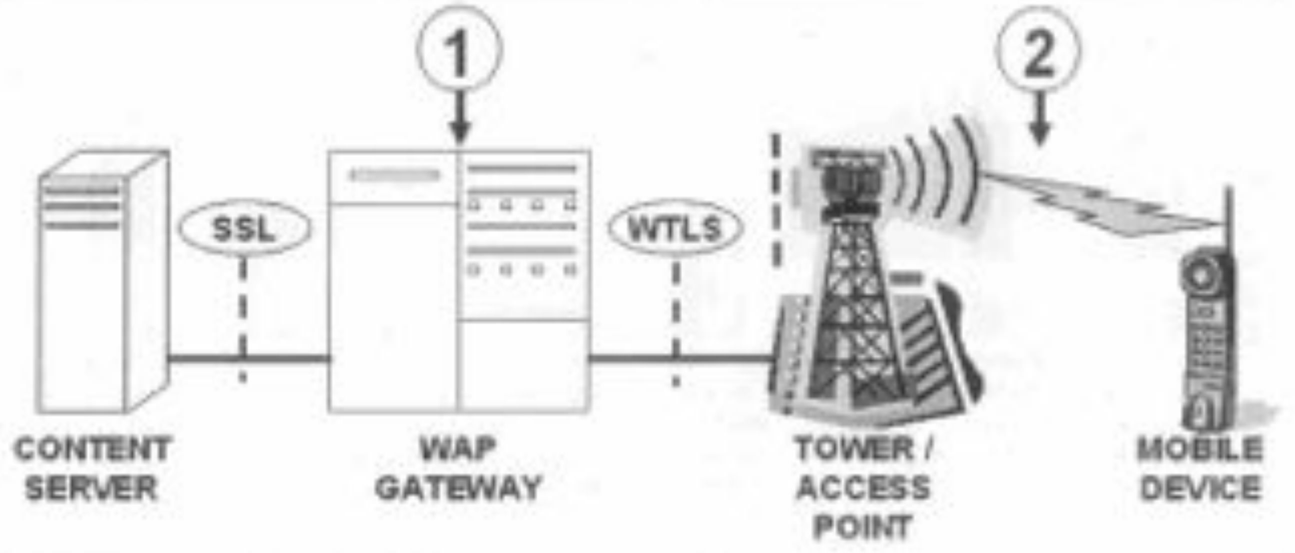
When asked about collectors maintaining the privacy of personal information, 93.2% and 90.4% of respondents are concerned for business and for government respectively (UCLA Center for Communication Policy, 2001). Several reasons specific to business were cited for privacy concerns, as outlined in Figure 7.

Privacy Issues in M-Commerce

The privacy concerns that are exhibited by e-commerce customers are also applicable to m-commerce customers. In addition, some new concerns arise in terms of security and privacy that are consequences of the lower security levels of wireless networks and the potential of using tracking and profiling technologies to offer m-customers unsolicited location-based services. These issues are explored below in some detail.

Wireless security. As discussed, security is not synonymous with privacy, but it is a critical element in preserving identifiable information as private. Although wireless networks present several advantages, including cost-effectiveness and convenience, a higher risk for a network security breach is present compared to wired networks. Figure 8 illustrates a typical flow of data during a wireless communication. The entities displayed are a user's mobile device from which communication is initiated or terminated; a communication tower (or access point) which acts as the transmitter or receiver of data; the WAP gateway (or WAP proxy) that is responsible for the conversion of data from a wirelessly encrypted state to one under a wired encryption mechanism and vice versa; and the Web server on which the content resides. WAP is the protocol that enables communication over a wireless network, similar to what HTTP is responsible for on a wired network. As for encryption, the wired encryption mechanism is a secure

Figure 8
Required Infrastructure for WAP Wireless Telecommunication



socket layer (SSL), whereas the wireless counterpart is wireless transport layer security (WTLS). The points labeled "1" and "2" in Figure 8 are a hacker's two main attack points.

Point 1 refers to where the "Two-Zone problem" or the "WAP Gap" occurs. The WAP architecture requires an intermediate gateway (WAP gateway) that encodes and decodes data from an SSL to a WTLS encryption format. This process is brief (milliseconds), but the data is unsecured in the interim, as it needs to be decrypted from WTLS into plain text and then re-encrypted into SSL. The inherent risk is loss/exposure of data if a hacker is able to extract the plain text (Gururajan, 2002). This problem is addressed effectively in devices accessing GSM networks as these devices handle the conversion from WTLS to SSL internally on the subscriber identity module (SIM) card, and therefore minimize the risk of a hack attack and improve overall performance as air time required for conversion is reduced. Other options are explored through new technologies, including wireless identification module (WIM) cards that are similar in functionality to SIM cards for non-GSM phones, and J2ME-enabled handsets, which allow the handset to send and receive content directly to and from the HTML server, respectively, without the need for an intermediate gateway (Schwartz, 2000).

Point 2 refers to the data stream that is carried through air and is susceptible to "eavesdropping". The success of the hacker in such an attempt depends in part on the encryption algorithm used. This is one security element that requires improvement. The GSM standard A5 algorithm utilizes a 54-bit encryption, which is slightly better than the IEEE 802.11 standard RC4-40 algorithm that only uses a 40-bit encryption. However, both are still not efficient to desired levels (Bank, 2001; Pesonen, 1999). The IEEE standard is more commonly known as wired equivalent privacy (WEP). When comparing this level of encryption to the respective levels of wired encryption at 128-bits, it becomes apparent how low the level of wireless security currently is, especially when one considers that hacking a 128-bit encrypted message is also feasible. In addition, implementing an effective encryption algorithm is further complicated due to the mobile device limitations that are still prevailing. Limited battery life, low processing memory, and even billing methods (i.e., per-minute pricing) act against the implementation of a 128-bit encryption algorithm in a wireless setting. Currently, a 128-bit encryption key would result in increased power consumption, longer waiting periods for each data exchange, and consequently, higher bills for the mobile user. For example, if Secure Sockets Layer (SSL) standards are used, approximately 45 seconds are required to establish a secure connection. This comes at a cost to the user, who will possibly be required to pay for the respective airtime (Schwartz, 2000).

To address some of these security issues, the IEEE will likely set the standard to the new advanced encryption standard (AES) in the near future (Fisher, 2001). However, despite the superiority of AES as an encryption standard, due to investments in products configured to work with WEP by wireless networking vendors, it is likely that along with a new technology called "fast packet keying", WEP will satisfy short-term wireless LAN security needs, and AES is likely to be part of long-term wireless LAN security solutions (Cam-Winget, Walker, Aboba, & Kabler, 2001). Fast packet keying addresses the vulnerability of an attacker's current ability to sniff a small number of packets on a WLAN and then guess the private encryption key that is being used (Fisher, 2001).

Aside from identifying the most likely points of a hack attack, it is important to address the loss or theft of a mobile device as a security issue, since the data stored in the device could be highly sensitive. A recent report in the UK found that 2,900 laptops, 1,300 PDAs, and over 62,000 mobile phones were left in London cabs over the first six months in 2001 (Middleton, 2001). To combat this situation, mobile users should be empowered through added features for their mobile devices that would safeguard their privacy. These features may be invisible to the user (e.g. memory protection, file access control) or they may require interaction (e.g. log in software, biometrics) (Gururajan, 2002; Johnson, 2002).

Tracking/profiling. In an e-commerce environment, tracking refers to the ability to monitor and trace current and previous consumer behaviour based on interactions with an on-line business. A popular example of Internet tracking technology for the purpose of profiling users is the use of cookies. Cookies are programs that are usually associated with specific Websites and store text files on the user's PC, so that information is stored and transmitted when the user revisits the associated sites. This information, which usually involves identifying the user's on-line activities (e.g. sites visited, duration of stay per page), is used by companies in their efforts to better understand their customers' preferences and needs. This constitutes a component of an effective customer relationship management (CRM) strategy. The wireless medium becomes an even more significant tool for enhanced CRM because of two characteristics. First, a mobile device is a personal item, therefore any information stored or activity performed can be credited to a single user, an advantage over home PCs, the user of which could be any member of the family. Second, there is an inherent capability of locating mobile devices, a capability known as location service. Building on the strength of location service, location-based services (LBS) are those that can be offered based on location of the mobile device through the use of indexing and guidance services. LBS enable mobile users to locate not only geographic locations, services, and products, but also other mobile users. Essentially, LBS become navigation services allowing mobile users to find their own position, the position of the desired location or site, the available modes of transport in reaching the desired location, and the location of other individuals (Raino, 2001). LBS can be achieved through the use of the following various technologies:

1. Satellite positioning, achieved through the use of a global positioning system (GPS) module that can be embedded in any mobile device. Via GPS satellites, the location of a mobile device can be determined within 20 metres with 95% reliability (Cavoukian & Gurski, 2002); however, current GPS modules consume power relatively heavily, and landscape, such as tall buildings or covered areas (e.g. parking garages), can affect GPS performance.
2. Network positioning, also known as cell positioning, works only with cellular phones. Although this service is feasible even in dense urban areas, it is not as accurate as GPS, nor is it likely to be free, since participation of the telecommunication operator is required.
3. Network-assisted satellite positioning, also known as A-GPS, is a hybrid of the previous two technologies, which addresses GPS landscape issues while improving the accuracy of location data.

To make use of the above technologies, device manufacturers will need to produce appropriately enabled devices. Several such devices will hit the market this year in North America, while in Europe they are already in use. Several applications lend themselves well to positioning systems, including emergency services (e.g. 911 in North America, 112 in Europe), roadside assistance, fleet management, information retrieval and advertising, mapping and routing, and locating friends.

Regional penetration rates are about to change, as a result of an FTC mandate (E911, Telecommunications Act, 1996) in the U.S., which requires wireless network carriers to locate the origin of a call within a specified distance. Japan had led the pack by implementing simple GPS solutions since 1999, but because of E911, by 2007 the US will account for more than half of the global market, with Asia in second place, and Europe in third (Allison, Moss, & Jaffery, 2001).

Positioning services provide additional information companies could use to improve understanding of the mobile user. The ability, however, to know the exact whereabouts of a mobile user may be perceived by the consumer as threatening, as this information could be dangerous if intercepted. Examples of such fears include (a) knowing where mobile users are makes it easier for them to become victims of physical attacks; (b) knowing that the residents of a home are away makes their residence vulnerable; and (c) location-based advertising that targets consumers based on their geographic location.

The last example, location-based advertising, is one of the most controversial aspects of the ability to track a mobile device and hence its user. Companies are using this ability to market their products/services more aggressively. An additional consumer concern is that this marketing will come at a cost to the mobile user, who may possibly end up paying to read or listen to an incoming advertising message that may be in the form of an e-mail message, SMS, or a phone call.

Privacy Legislation in Canada

Countries around the world are dealing with privacy differently; however, there are two examples of a set of guidelines being adopted by a number of countries. First, the Organisation for Economic Co-operation and Development, with its 29 member countries, is focusing on promoting an internationally coordinated approach to privacy policy making for global networks. Second, the European Union (EU), and specifically the European Commission, has established a Directive on Personal Data Protection (Directive 95/46/EC) (European Commission, 1999). Common rights granted to citizens of these countries include: (a) the right to know the source of personal data processing and the purposes of such processing; (b) the right to access and/or rectify inaccuracies in own personal data; and (c) the right to disallow the use of personal data.

In the United States, the Federal Trade Commission (FTC) has implemented the Children's Online Privacy Protection Act (2000) and has outlined a policy similar to that of the EU, but it has not been presented to Congress, as the focus in the U.S. is on self-regulation (Head & Yuan, 2001).

In Canada, great strides are being made on privacy legislation with the intent of matching or coming close to matching the EU Directive. Currently, Canadians are protected at several levels to different extents: federal, provincial, private, and sector-specific (Privacy Commissioner of Canada, 2002). At the federal level, there are two privacy laws: the Privacy Act and the Personal Information Protection and Electronic Documents Act. The Privacy Act was implemented on July 1, 1983, and places limitations on the collection, use, and disclosure of personal information by federal government departments and agencies. In addition, the Privacy Act grants Canadians the right to access and correct personal information stored about them that is maintained by these federal government organizations. The Personal Information Protection and Electronic Documents Act (Bill C-6) was implemented as of January 1, 2001. Bill C-6 outlines how private sector organizations may collect, use, or disclose personal information in their business operations. As of January 1, 2002, Bill C-6, similar to the Privacy Act, enables individuals to access and correct any personal information that a business acting on a federal level maintains about them, as well as any personal health information that is collected, used, or disclosed by organizations. The final stage of Bill C-6 is to be implemented on January 1, 2004. This stage will address the collection, use, or disclosure of personal information during any business operation within a province, including provincially regulated organizations. Violation of both Acts and/or other privacy-related complaints is taken up by the Privacy Commissioner of Canada.

At the provincial level, privacy legislation on the collection, use, and disclosure of personal information held by government agencies is in place, except for Prince Edward Island and Newfoundland. On the private sector level, currently only Quebec has passed a personal data protection law (Bill 68) that applies to the provincially regulated private sector. This law, building on already existing regulation of the collection, use, and disclosure of personal information held by credit bureaus, insurance companies, pharmacies, and any other commercial enterprise, also grants Quebecers the right to access and correct personal information. Hence, Quebec now has the highest level of privacy protection in North America.

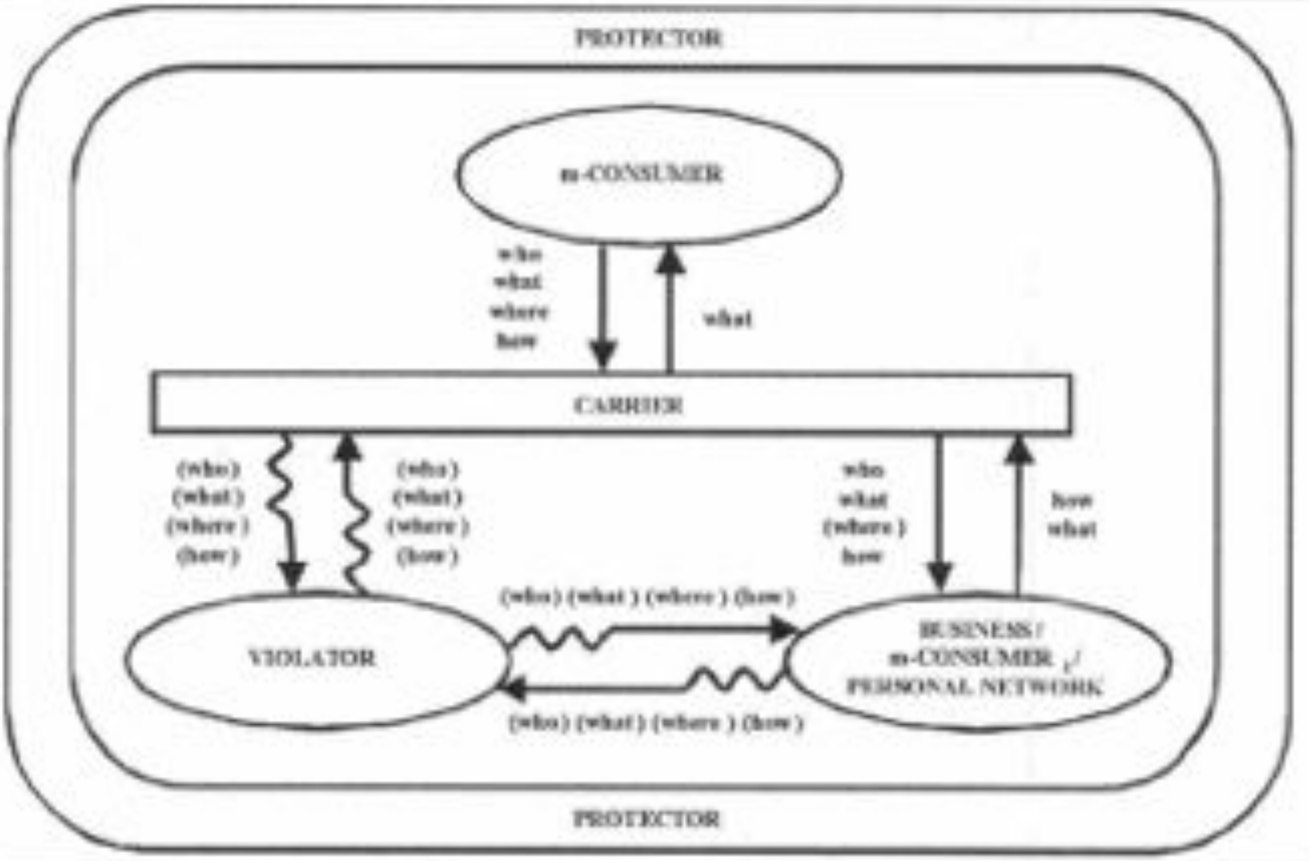
With respect to specific sectors, Alberta and Manitoba have enacted, while Ontario and Saskatchewan intend to enact, legislation that deals with the collection, use, and disclosure of personal health information by provincial health care organizations and other approved individuals and agencies. In addition, the federal Bank Act regulates the use and disclosure of personal financial information by federally regulated financial institutions. Similar restrictions are in place for financial institutions, such as credit unions and insurance companies, that fall under provincial jurisdiction.

Finally, various consumer protection laws at both the federal and provincial levels offer limited protection against illegal and unethical business practices that may constitute an infringement of privacy. Some provinces have privacy tort laws, which provide a civil remedy for a subject whose privacy has been violated.

An Interaction Framework for Wireless Privacy

A theoretical framework for privacy protection in e-commerce has been proposed (Head & Yuan, 2001); however, no such framework has been introduced for m-commerce. The e-commerce privacy framework introduced by Head and Yuan identifies the following four key players and outlines their interactions in the context of privacy violation and protection within an e-commerce environment: (a) the *subject*, who wishes to control the

Figure 9
Wireless Privacy Interaction Framework



Note: Data without parentheses must be passed between indicated parties, while data within parentheses are optionally passed.

distribution of personal information to collectors; (b) the *collector*, who wishes to collect private information for business purposes; (c) the *violator*, who illegally or unethically acquires, stores, sells, or uses the subject's private information; and (d) the *protector*, who attempts to ensure the subject's privacy rights by stopping the violator and providing guidelines for the collector.

As outlined in the second and third sections of this paper, wireless communication entails new modes of interaction and associated consumer concerns, resulting in distinct privacy issues and problems. Therefore, we propose a new wireless privacy interaction framework, as shown in Figure 9, which reflects the nature of interactions within a wireless environment. In the context of the new framework, we identify the following players:

1. The *m-consumer* corresponds to the privacy subject introduced above (Head & Yuan, 2001).
2. The *carrier* enables communication between the m-consumer and other parties. Carriers play a critical role as enablers for wireless interactions and as such they are in a position to collect rich and private information about the m-consumer (e.g. location). By virtue of the role it plays, the carrier could correspond to the collector in the Head and Yuan (2001) framework.
3. The *business/m-consumer/personal network* are parties or entities with which the m-consumer wishes to communicate. The business party corresponds to the collector in the Head and Yuan (2001) framework. The m-consumer and personal network correspond to the entities identified by the same name in the Coursaris and Hassanein (2002) framework for m-consumer interaction modes within a wireless environment.
4. The *violator* corresponds directly with the violator described above (Head & Yuan, 2001).
5. The *protector* corresponds directly with the protector described above (Head & Yuan, 2001). Protectors may be the government or third party self-regulatory bodies

(e.g. industry associations, privacy protection groups, certification programs, watchdogs, and anonymity services).

As Figure 9 outlines, there are four types of information that can be collected and passed through wireless communication: (a) *who* refers to the identities of the sender and/or receiver; b) *what* refers to the content being communicated; (c) *where* refers to the location of the m-consumer; and (d) *how* refers to the device being used by the sender and/or receiver. For example, considering an interaction between the m-consumer and a business, the m-consumer may initiate the communication by sending the carrier information about his/her identity (e.g. IP address) and the identity of the business (who), the content of the communication (what), the type of device being used for the communication (how) and the current location of the m-consumer (where). The carrier then passes the who, what, and how information to the business. The carrier could also choose to send location-based information (where) to the business. However this should ideally only be performed with the consent of the m-consumer. The business, in turn, responds by providing the requested content (what) to the appropriate m-consumer (who) via the carrier.

In this framework, the violator may seek to gain illegal or unethical access to the m-consumer data (who, what, where, and how) via the carrier or directly through the various entities the m-consumer interacts with. Figure 9 represents the activities of the violator by *crooked or jagged* arrows. The protector encircles the interactions in this framework, since the protector must interact with all the parties to safeguard the m-consumer's privacy rights. For example, the government's role in m-consumer privacy protection includes providing guidance and boundaries for the activities of carriers, businesses, and other m-consumers. The government also provides warnings and legal consequences to privacy violators. Third-party self-regulatory bodies also serve as protectors. For example, privacy protection groups may assist wireless parties through education, certification programs encourage the collectors to adhere to acceptable privacy guidelines, privacy watchdogs monitor and publicize acts of privacy violation, and anonymity services offer the m-consumers the ability to block some of their personal identity.

Having identified the privacy parties and the types of information exchanged between them in a wireless environment, we can now analyse the responsibilities of the various parties towards protecting the privacy of the m-consumer. Table 3 details these responsibilities of the privacy parties. This table also serves to help link the data movement within the Wireless Privacy Interaction Framework (Figure 9) with associated party-to-party responsibilities in any data exchange. This can be accomplished by examining the corresponding cells between the exchanging parties in Table 3.

Discussion

As we have already discussed, the main ingredients necessary to protect one's right to control the flow of information about themselves over wireless networks are privacy, security, and legislation. Consumer privacy may be effectively protected only if the issues related to these three areas are addressed and education is used as a catalyst. Consequently, there are implications for each of the parties identified in the wireless privacy interaction framework (Figure 9) that are described below.

M-consumers are concerned with their privacy, which in m-commerce extends from the information context to also include consumers' physical space. As such, the concern is escalated compared to the level of privacy concern for e-commerce. Consumers need to be armed with knowledge about their responsibilities, business' information practices, and possible courses of action in the event of privacy violation. Unfortunately, a survey of IT security professionals in the United States identified the lack of end-user awareness as the primary obstacle to achieving adequate information security levels (Foran, 1996). Thus, the fundamental requirement here is for consumers to learn about privacy and security measures, and to adjust security and privacy settings on their wireless devices to their satisfaction. Second, consumers should review a company's privacy policy—in which full disclosure should be given on how personal information will be used—and decide accordingly whether to interact with that business. In the event that a privacy violation takes place, action should be taken to bring the violators to light, since lack of exposure of a violation may lead to a series of attacks before the violator is stopped.

Businesses, including network carriers, are faced with the issue of confidentiality. Confidentiality is an obligation of the owner of information (business) to protect the personal information of a subject (m-consumer) with which it has been entrusted. A promise of confidentiality is a duty to maintain the secrecy of the information and not misuse or wrongfully disclose it. Confidentiality establishes a bond of trust between the consumer and the business that becomes particularly important in m-commerce, because of the escalated privacy concern. Extending from this promise, security is a critical requirement. A security breach is less the hackers' success and more the business' failure to set up proper defense systems. Consequently, a business' primary responsibility is to implement security measures to pre-

Table 3
Wireless Privacy Party-to-Party Responsibilities Matrix

	m-Consumer	Carrier	Business	m-Consumer$_j$	Violator	Protector
m-Consumer	• educate oneself about privacy and security issues and regulations • implement adequate measures to protect the security and privacy of personal data • protect wireless device against loss or theft	• examine privacy policy • exercise caution when sharing data • make decisions to opt in or opt out of specific services • demand adequate privacy and security protection • adhere to any applicable carrier-recommended privacy or security guidelines	• examine privacy policy • make decisions to opt in or opt out of specific services • exercise caution when sharing data • verify data quality • demand adequate privacy and security protection • adhere to any applicable business-recommended privacy or security guidelines	• exercise caution when sharing data • share knowledge about privacy and security issues • protect wireless device against loss or theft	• implement adequate measures to prevent violations • promptly act on and report any violations	• educate oneself about the various privacy protectors and their roles / jurisdiction • demand adequate protection or enforcement • promptly act on and report any violations
Carrier	• share privacy policy • provide opportunity to opt in or opt out of specific services • provide adequate privacy and security protection • promptly report any potential violations	• educate oneself about privacy and security issues and regulations • develop, implement, and share a privacy policy • self regulate	• only share consumer-consented data • ensure business partners adhere to appropriate privacy guidelines	• only share consumer-consented data	• implement adequate measures to prevent violations • promptly act on and report any violations	• work with protector to develop privacy policy • be aware of and abide by privacy regulations imposed by protectors • promptly act on and report any violations • support auditing procedures and comply with auditing recommendations
Business	• share privacy policy • provide opportunity to opt in or opt out of specific services • ensure data quality • provide adequate privacy and security protection • promptly report any potential violations	• adhere to carrier-recommended privacy guidelines	• educate oneself about privacy and security issues and regulations • develop, implement, and share a privacy policy • self regulate	• only share m-consumer consented data	• implement adequate measures to prevent violations • promptly act on and report any violations	• work with protector to develop privacy policy • be aware of and abide by privacy regulations imposed by protectors • promptly act on and report any violations • support auditing procedures and comply with auditing recommendations

Table 3 — continued

Wireless Privacy Party-to-Party Responsibilities Matrix

	m-Consumer	Carrier	Business	m-Consumer$_j$	Violator	Protector
m-consumer$_j$	• share knowledge about privacy and security issues and regulations • honour privacy and security requests of m-consumer • promptly report any potential violations • protect wireless device against loss or theft	• adhere to any applicable carrier-recommended privacy or security guidelines	• only share m-consumer consented data	• educate oneself about privacy and security issues and regulations • protect wireless device against loss or theft	• implement adequate measures to prevent violations • promptly act on and report any violations	• educate oneself about the various privacy protectors and their roles / jurisdiction • demand adequate protection or enforcement • promptly act on and report any violations
Violator	• refrain from violating personal privacy	• refrain from attacking the carrier's network • refrain from intercepting communications with the m-consumer	• refrain from attacking the business' network • refrain from intercepting communications with the m-consumer	• refrain from attacking the m-consumer's network • refrain from intercepting communications with the m-consumer	• educate oneself about privacy and security issues and regulations	• be aware of and abide by privacy regulations imposed by protectors
Protector	• seek information about m-consumer privacy concerns • educate about privacy and security issues and regulations • investigate suspected privacy violations • publicize any identified privacy violations • provide legal protection against violations • provide anonymity services	• educate about privacy and security issues and regulations • work with carrier to develop privacy policy • provide certification services • monitor compliance with privacy policies, certification requirements and regulations • investigate suspected privacy violations • publicize any identified privacy violations	• educate about privacy and security issues and regulations • work with business to develop privacy policy • provide certification services • monitor compliance with privacy policies, certification requirements and regulations • investigate suspected privacy violations • publicize any identified privacy violations	• seek information about m-consumer privacy concerns • educate about privacy and security issues and regulations • investigate suspected privacy violations • publicize any identified privacy violations	• educate about privacy and security issues and regulations • publicize any identified privacy violations • enforce legislation against privacy violators	• educate oneself about continuously evolving privacy and security issues and regulations • self-regulate

vent any possible breaches and violations. Also, a business needs to implement a clear and complete privacy policy according to the standards specified by the Personal Information Protection and Electronic Documents Act (PIPEDA) (Privacy Commissioner of Canada, 2000). Finally, the issue of industry standards arises when consumers are stack between two misaligned privacy policies of partnering organizations. For example, when a mobile phone user leaves his/her area of coverage and is using a partner carrier's network, he/she is no longer protected by the privacy policy of their operator. Instead, the partner carrier's policy is in effect, which may be less or more comprehensive. In this case, due to the different network carrier policies, a consumer's private information may be used without consent. The same issue arises among any business partners. Hence, standardization in the m-commerce industry is required to prevent such complications. Canada is in a good position to see through such a wireless privacy standardization initiative since there are only four wireless network operators. However, for the rest of the wireless market players, such as m-tailing (wireless retailing), standardization may be a lot more difficult to achieve and reliance on legislation or self-regulation may be the only answer.

Self-regulation is particularly favoured, since it places the onus on businesses within the same industry to develop, implement, and enforce policies. This is advantageous since the government may not be well suited to understanding the specifics for each industry when developing new legislation. Instead, self-regulation promises to yield a more realistic, practical, and accepted framework by which business may abide. Such self-regulations must be within the general guidelines specified by provincial and federal legislation.

Protectors are faced with developing and enforcing policies and legislation to protect consumer privacy. Canada was slow to react to privacy concerns compared to the progress made in Europe. It was only in the mid-1990s that the first case of hacking was prosecuted under the Canadian Criminal Code. Prior to that, and for many years, hackers operated without fear because no law existed (Foran, 1996). Today, with the second phase of the federal act (PIPEDA) in place, and the third and final phase scheduled for January 1, 2004, Canada has come a long way in safeguarding a citizen's right to privacy. The privacy standards set in PIPEDA were derived from the Canadian Standards Association's (2001) *Model Code for the Protection of Personal Information*. This was a joint effort between business, government, and consumers, and therefore the protection measures outlined are comprehensive. Still, current legislative structure includes two components that could be problematic. First, an issue would emerge in the event a province decides to adopt legislation that is not aligned with the federal privacy legislation. Although that scenario is not probable it is a possible area of conflict and frustration for the consumer. Most provinces have so far passed their respective laws modeled after PIPEDA and, in the event that a province does not put into place equivalent legislation by January 1, 2004, all remaining private sector enterprises will be covered by the federal statute (Reid, 2001). A second and more important situation arises when the government deals with third parties who have not adopted privacy policies similar to those of the government. One such example exists in health care. Specifically, when a two-tier health care system is in place, information privacy is potentially at risk. In this case, public health care records (e.g. at a hospital) get transferred to private clinics upon request. Although hospitals and other public care facilities fall under the current PIPED Act, the private practices currently do not. Hence, a grey area arises in protecting what might arguably be the most personal of information. Finally, the protector has the responsibility of educating the other m-commerce market players on relevant issues and measures in place.

The only effective approach to deal with these and any future issues in this area is to ensure collaboration with, not isolation from, each of the m-commerce market players. It is also important to monitor developments in the area of wireless privacy in other regions around the world, and in particular those with higher m-commerce penetration. This would facilitate a proactive approach to dealing with such a critical issue for the m-commerce industry.

Conclusion and Future Research

Mobile commerce (m-commerce) is a natural extension of electronic commerce (e-commerce) and represents a new channel through which users can interact wirelessly with other people or businesses. This provides m-consumers with significant convenience and flexibility through an anytime/anywhere mode of interaction.

The Canadian market, in particular, may be well positioned for the successful adoption of m-commerce applications. Canadians are becoming increasingly open and positive in their acceptance of new technologies, such as the Internet and e-commerce. In addition, the Canadian government is in favour of implementing regulatory policies that will help smooth the transition from wired to wireless communications. Canada is also in a strong position to make such a transition due to the increasing availability of affordable wireless services and products offered through four major carriers.

However, there are several areas of concern associated with m-commerce that need to be addressed for it to realize its full potential, in Canada or elsewhere. In particular, we have identified a more acute level of security and privacy concerns for consumers within wireless environments compared to wired environments.

Based on an investigation of m-commerce and associated privacy issues, we have introduced a new interaction framework for wireless privacy. This framework serves to identify the interacting parties within the m-commerce environment and provides these parties with a clearer understanding of the information that is exchanged during a wireless interaction with associated corresponding risks. This framework also provides the basis for the wireless privacy party-to-party responsibilities matrix we have presented, which clarifies the responsibilities of various parties towards enhancing the privacy of the m-consumer throughout all segments of wireless interactions.

Businesses hoping to take advantage of this potentially lucrative market must strive to fully understand the concerns of the m-consumer regarding privacy and security, so as not to repeat the same mistakes that led to the slowdown in e-commerce success. Privacy, security, and legislation combined with education can facilitate strong privacy protection practices, maintaining the consumer's interest while benefiting all m-commerce market players.

While this paper presents a useful discussion and framework for understanding m-commerce issues, focusing on wireless privacy, several topics in this area still require a thorough investigation. In order for m-commerce to realize its full potential, we must investigate and devise business models that take full advantage of the rapidly evolving technology improvement in the areas of wireless networks, devices, and protocols. It is critical that such m-commerce business models focus on satisfying the needs of the m-consumer while minimizing their concerns. Research is also needed in the area of m-commerce usability. As with e-commerce, usability is critical to the success of m-commerce applications. In particular, the nature of m-commerce devices requires new usability research that focuses on re-purposing content in a very limited display area. Usability will greatly determine the fate of m-commerce adoption by consumers. Lastly, the framework developed in this paper is general, but should be well suited to work in any industry. However, this framework should be scrutinized, and potentially modified, in the context of specific industries (such as the health or financial sectors) to reflect their particular privacy parties and protection needs.

M-commerce is an emerging market that relies on technologies that are still rapidly evolving. New privacy concerns may materialize in conjunction with these developments, while existing ones will continue to represent major issues for m-consumers. As m-commerce evolves, it is critical to remember that wireless privacy protection is the responsibility of all the parties involved in this market.

References

Accenture. (2001). The future of wireless: Different than you think, bolder than you imagine. [On-line] http://www.accenture.com/xdoc/en/ideas/isc/pdf/Future_of_Wireless.pdf

ACNielsen. (2000). ACNielsen study indicates Canadian PC ownership now more than 60 percent. [On-line] http://www.acnielsen.com/news/american/ca/2000/20000127.htm

Agranoff, M.H. (1993, Summer). Controlling the threat to personal privacy. *Journal of Information Systems Management*, pp. 48-52.

Allison, C., Moss, J., & Jaffery, N. (2001). Wireless location technologies: Options for E-911 and beyond. [On-line] http://www.wowcom.com/market_research/documents/1270-01_ExSum.pdf

Bask, J. (2001). Pervasive computing: Travel and business services. Telecommunications Software and Multimedia Laboratory. [On-line] http://www.tml.hut.fi/Studies/Tik-111.590/2001s/papers/joni_bask.pdf

Cam-Winget, N., Walker, J., Aboba, B., & Kahler, J. (2001). Rapid re-keying WEP a recommended practice to improve WLAN security. IEEE. [On-line] http://www.drizzle.com/~aboba/IEEE/

Camp, L.J. (1999). Web security and privacy: An American perspective. *Information Society: An International Journal, 15* (4), 249-256.

Canadian Standards Association. (2001). Model code for the protection of personal information. [On-line] http://www.csa.ca/standards/privacy/default.asp?load=code&language=English

Canadian Wireless Telecommunications Association (CWTA). (2002). Wireless facts and figures. [On-line] http://www.cwta.ca/industry_guide/facts.php3

Cavoukian, A. & Gurski, M. (2002). Privacy in a wireless world. Information and Privacy Commission of Ontario.

Cole, C. (2001). 5 things I want from my mobile. *m-Commerce World*. [On-line] http://www.internetworld.co.uk/mcomm/vRoom/articles/article.cfm/B6D4ACE6-D1D4-11D4-BEE900B0D0A143DF

Coursaris, C. & Hassanein, K. (2002). A framework for m-commerce: A consumer's perspective. 3rd World Congress on the Management of Electronic Commerce. Hamilton, ON.

Daum, A. (2001). Mobile consumers: What do they want? How much will they pay? GartnerG2.

European Commission. (1995). Directive 95/46/EC of the European Parliament. [On-line] http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

Fisher, D. (2001). WLAN security in neutral. *eWeek*. [On-line] http://www.eweek.com/article/0,3658,s%3D701%26a%3D20541,00.asp

Foran, B. (1996). Censorship and privacy issues for law enforcement. 91st Annual Canadian Association of Chiefs of Police Conference. [Online] http://privcom.gc.ca/speech/archive/02_05_a_960826_e.asp

Gurunajan, R. (2002). Mobile computing: Security risks. 23rd World Congress on the Management of Electronic Commerce, Hamilton, ON.

Head, M.M. & Hassanein, K. (in press). Trust in e-commerce: Evaluating the impact of third-party seals. *Quarterly Journal of Electronic Commerce*.

Head, M.M. & Yuan, Y. (2001). Privacy protection in electronic commerce: A theoretical framework. *Human Systems Management, 20*, 149-160.

Ipsos-Reid (2001). The face of the Web. [On-line] http://www.ipsos-reid.com/media/dsp_displaypr_cdn.cfm?id_to_view=1229

Johnson, D. (2002). Securing your PDA. *IDG.net*. [On-line] http://www.idg.net/ic_794581_5056_1-2887.html

Keyte, C. (2001). It's not about the phones! *M-commerce World*. [On-line] http://www.internetworld.co.uk/mcomm/vRoot/articles/article.cfm/A0154418-21C5-11D5-A04E00C04FA0E16A

Koster, E.H. (1999, May). Zero knowledge: Personal data on the Internet. *The Computer Lawyer*. [On-line] http://www.oppenheimer.com/intprop/news/zeroprivacy.shtml#worth

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G., & Wolff, S. (2002). A brief history of the Internet. *Internet Society* [On-line] http://www.isoc.org/internet/history/brief.shtml

Little, J. (2001). M-commerce. Amazing! *CJRW*. [On-line] http://www.cjrw.com/amazing/mcommerce.html.

Manley, J. (1998). Canada-Europe Parliamentary Association of the Council of Europe.

McGinity, M. (2000). Bumpy road ahead for m-commerce. *Inter@ctive Week*. [On-line] http://www.zdnet.com/intweek/stories/news/0,4164,2445298,00.html

Middleton, J. (2001). Lost mobile devices drive security fears. *vnunet.com*. [On-line] http://www.vnunet.com/News/1125076

Morrison, D. (2001). Technology push and customer pull: The wireless Internet comes of age. Presentation at McMaster University, Hamilton, ON.

NCR Corporation. (2003). Teradata personal data protection principles. [On-line] http://www.teradata.com/main/privacy.asp

Nielsen, J. (2000). *Designing Web usability: The practice of simplicity*. Indianapolis, IN: New Riders Publishing.

Peck, A. (2001). WAP's summer of discontent. *M-commerce world*. [On-line] http://www.internetworld.co.uk/mcomm/vRoot/articles/article.cfm/87DB2C1B-D4FC-11D4-A9E300C04FA0E16A

Pesonen, L. (1999). GSM interception. Telecommunications Software and Multimedia Laboratory. [On-line] http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/gsminterception/netsec.html

Pocket Directory. (2001). Smart phones. [On-line] http://www.pocketdirectory.com/hardware/hproducts.aspx?idCat=4&selHId=1

Privacy Commissioner of Canada. (2000). Statutes of Canada 2000. [On-line] http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp

Privacy Commissioner of Canada. (2002). Privacy legislation in Canada 2002. [On-line] http://www.privcom.gc.ca/fs-fi/fs2001-02_e.asp

Raisio, A. (2001). Location-based services and personal navigation in mobile information society. New Technology For A New Century – Technical Conference, Seoul, Korea. [On-line] http://www.fig.net/figtree/pub/proceedings/korea/full-papers/pdf/plenary1/raisio.pdf

Reid, Hon. J.M. (2001). Remarks to security and privacy for government on-line conference. [On-line] http://infocom.gc.ca/speeches/speechview-e.asp?intspeechId=5

Rogers Communications. (2002). Network coverage info. [On-line] http://www.shoprogers.com/store/wireless/coverage/overview.asp?shopperID=85XT109NSK9Q2JE2100J74HJFP4PK5ME0

Schwartz, E. (2000). Fixing a security hole when the rain gets in: Two-zone encryption limits wireless usage. *InfoWorld*. [On-line] http://www.infoworld.com/articles/op/xml/00/12/04/001204opwireless.xml

Statistics Canada. (2001). The 2000 household Internet use survey. [On-line] http://www.statcan.ca/Daily/English/010726/d010726a.htm

UCLA Center for Communication Policy. (2001). The UCLA Internet report 2001: Surveying the digital future. Los Angeles: UCLA Center for Communication Policy.