m-Commerce in Canada: An Interaction Framework for Wireless Privacy[1]

Constantinos Coursaris, Khaled Hassanein & Milena Head

Michael G. DeGroote School of Business,
McMaster University,
1280 Main Street West
Hamilton, Ont., L8S 4M4
Canada

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.

Keywords: m-Commerce, e-Commerce, m-Consumer, wireless, privacy, security, Canadian, location based services, legislation.

1. Introduction

From the inception of the Internet and over the last two decades the Internet has undergone significant change. Although the Internet was designed before Local Access Networks (LANs) existed, it has adapted to suit new network technologies (e.g. client-server and peer-to-peer computing) and telecommunication services (e.g. 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 (i.e., laptop computers, two-way

[1] Coursaris, C., Hassanein, K., and Head, M. (2003). "m-Commerce in Canada: An Interaction Framework for Wireless Privacy", *Canadian Journal of Administrative Sciences*, 20(1), 54-73.

pagers, PDAs, cellular phones). The mobility associated 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 already having access to them (e.g. Japan). These networks are commonly referred to as IMT-2000 on a global scale, and regional implementations are uniquely named (e.g. CDMA2000 in North America, W-CDMA/ UMTS in Europe & Japan, cdmaOne in Japan).[2] 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 Personal Digital Assistants (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 that are capable of tasks ranging from e-mail retrieval 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 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 OECD[3], 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).

The 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. Section 2 continues with a discussion on the needs and concerns of the m-Consumer (mobile consumer)

[2] CDMA: Code-Division Multiple Access, W-CDMA: Wideband CDMA, & UMTS: Universal Mobile Telephony System.

[3] OECD: Organization for Economic Co-operation and Development.

and an overview of m-Commerce business applications, identifying privacy and security as key concerns. Section 3 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 Section 4, a wireless privacy interaction framework is introduced 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. Section 5 discusses the wireless privacy implications to the parties identified within the wireless privacy interaction framework. Finally, Section 6 provides some conclusions and potential directions for future research.

2. 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, Personal Digital Assistants (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 ways through which evolving customer needs could potentially be met.

The m-Commerce and the e-Commerce business environments and activities have a lot in common. This is the case 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, as well as 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 Local Area Network (LAN) while that for m-Commerce 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/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 & Communication Protocols:** Most people are familiar with the Hyper Text 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 (e.g. the Wireless Application Protocol (WAP) and DoCoMo's (Japan) proprietary protocol i-Mode). Different from the wired Web's Hyper Text 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.

2.1. 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 penetration 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 online (a growth rate of 81% since 1999). The subset of these households that actually made an online 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 online (i.e. researched and proceeded with purchase offline). The average expenditure per online 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 online 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 online last year, edging the US, who had 72%. It now appears that the United States (US) 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 centers (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 online 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 online 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 US 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 US 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 US. 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 fast evolving. 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:

- 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.
- Increasing affordability of wireless relative to wired usage.
- 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 satellite 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, 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) (Canadian Wireless Telecommunications Association 2002). Network coverage is critical in generating new subscriptions. Figures 6a through 6d show the wireless network coverage maps for each of the four major carriers. The shaded regions in these maps represent analog wireless coverage, whereas the dark region represents 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 Canadian live in the southern parts of Canada. Additionally, a large proportion of Canadians (85%) also have access to digital wireless services, which centre around the highly-populous metropolitan areas (Rogers 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 consequent of pressure exerted by competition.

2.2. 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. These needs are (Coursaris and 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. inter-operability 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), and may be carried out within 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 leisurely 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 within the m-Commerce environment. The main concerns are summarized below (Coursaris and Hassanein 2002):

- **Privacy:** In the information context, privacy refers to a user's fear of other people/organizations knowing what s/he 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, not replicated long articles from the wired

> Web (McGinity 2000). This notion ties in with usability, which raises the questions of 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 user frustration is experienced 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 for not only converting consumers to wireless Internet users, but also to retain these mobile users for the long run.

Canadian studies on ranking the above consumer 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 and Hassanein 2002). 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.

2.3. 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; according to which need they predominantly cater to. The characteristics identified for each business application in Table 2 include the following (Coursaris and Hassanein 2002): (i) Consumer needs addressed by the business application; (ii) Wireless Interaction modes covered by the business application; and (iii) Concerns associated with the business application.

The applications presented in Table 2 are those of highest interest to consumers (Daum 2001), 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, as well as, to engage in commercial transactions.

What is of particular interest here is the overlap that exists between the identified wireless applications that are 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 for 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:

- Communication: voice, e-Mail, chat, text messaging, data
- Information: 411, yellow pages, directions, updates (traffic, weather), travel deals, hotels, restaurants, taxi service, news (portals, business), agenda, address book
- Entertainment: Games, listings (movies, event, sports), horoscope, lottery, ring tones
- Commerce: Pay bills, stocks (trade, get quotes), check bank account balance, buy goods

The above services are available on digital networks (i.e. second-generation or "2G" and newer technologies). Future applications will be driven by the high bandwidth and associated high speed rates of third-generation (3G) technology. These applications will be targeting both consumers and businesses. For consumers the focus of applications developed may be focused 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:

- Payment: Store credit card or bank account information on a mobile phone and use it to purchase.
- Images: Store full colour photographs on a mobile device.
- Tracking: Identifying the location of a mobile user.
- Videoconferencing: Video and audio real-time feed can facilitate enhanced communication.
- Notification: Instant alerts (e.g. flight delay/cancellation)
- Search agents: Find 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.

3. 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). From the identified consumer concerns in section 2.2, privacy and security are always among the top concerns for consumers. Often the two concepts are even 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 and 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).

3.1. Privacy in e-Commerce

Consumer privacy concerns can be major inhibitors for e-Commerce success. These concerns revolve around several online privacy principles or notions that are outlined below (adapted from 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 only fulfill 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.
- ***Security***: Personal data must be protected against possible loss, unauthorized access or tampering.

However several data collectors are motivated to deviate from the above principles in search for 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 US 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 (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 online 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). Specifically for business, several reasons were cited for privacy concerns, which are outlined in Figure 7.

3.2. 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 consequent of the lower security levels of wireless networks and to the potential of using tracking and profiling technologies to offer m-customers unsolicited location based services. These issues are explored below in some detail.

3.2.1. Wireless Security

As discussed in Section 2, 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 initiates or terminates, 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 stands for Wireless Access Protocol and is the protocol that enables communication over a wireless network, similar to what HTTP (HyperText Transfer Protocol) is responsible for on a wired network. As for encryption, the wired encryption mechanism is SSL (Secure Socket Layer), whereas the wireless counterpart is WTLS (Wireless Transport Layer Security). 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. As seen in Figure 8, the WAP architecture requires an intermediate gateway (WAP gateway) that encodes and decodes data from an SSL to a WTLS encryption format. This process lasts briefly (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 SIM (Subscriber Identity Module) 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 WIM (Wireless Identification Module) 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 medium 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[4] 802.11 standard RC4-40 algorithm that only uses a 40-bit encryption. However, both are still not efficient to desired levels (Pesonen 1999; Bask 2001). The IEEE standard is more commonly known as WEP (Wired Equivalent Privacy). 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 AES (Advanced Encryption Standard) 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, Walker et al. 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 2900 laptops, 1300 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).

[4] IEEE: Institute of Electrical and Electronics Engineers.

3.2.2. Tracking/Profiling

Within an e-Commerce environment, tracking refers to the ability to monitor and trace current and previous consumer behaviour based on their interactions with an online 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 online activities (e.g. sites visited, duration of stay per page), is used by companies in their efforts to better understand their customers' preferences and/or 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 and therefore any information stored, as well as any activity performed, can be credited to a single user – this is an advantage over home PCs, as the user 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) refers to services 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, as well as the location of other individuals (Rainio 2001). LBS can be achieved through the use of the following various technologies:

- **Satellite positioning:** achieved through the use of a GPS (Global Positioning System) module that can be embedded in any mobile device. Via GPS satellites, the location of a mobile device can be determined within 20 meters with 95% reliability (Cavoukian and 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.

- **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.

- **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 is 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 US, 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 et al. 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 as threatening by the consumer, as this information could be dangerous if intercepted. Examples of such fears include:

- Knowing where mobile users are makes it easier for them to become victims of physical attacks.
- Knowing that the residents of a home are away makes their residence vulnerable.
- 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 email message, SMS, or a phone call.

3.3. 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 Organization for Economic Co-operation and Development with its 29 member countries are 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 the following:

- The right to know the source of personal data processing and the purposes of such processing.
- The right to access and/or rectify inaccuracies in own personal data.
- The right to disallow the use of personal data.

In the United States (US), 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 US is on self-regulation (Head and 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 1st, 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 1st, 2001. Bill C-6 outlines how private sector organizations may collect, use or disclose of personal information in their business operations. Similar to the Privacy Act, and as of January 1st, 2002, Bill C-6 enables individuals to access and correct any personal information 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 1st, 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 has 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.

4. An Interaction Framework for Wireless Privacy

A theoretical framework for privacy protection in e-Commerce has been proposed (Head and Yuan 2001), however no such framework has been introduced for m-Commerce. The e-Commerce privacy framework introduced by Head and Yuan (2001) identifies the following four key players and outlines their interactions in the context of privacy violation and protection within an e-Commerce environment:

- *The Subject*: who wishes to control the distribution of personal information to collectors;
- *The Collector*: who wishes to collect private information for business purposes;
- *The Violator*: who illegally or unethically acquires, stores, sells, or uses the subject's private information; and
- *The Protector*: who attempts to ensure the subject's privacy rights by stopping the violator and providing guidelines for the collector.

As outlined in Sections 2 and 3, 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. Within the context of the new framework, we identify the following players:

- *The m-Consumer*: who corresponds to the privacy *subject* introduced above (Head and Yuan 2001)
- *The Carrier*: who 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 & Yuan framework (Head and Yuan 2001).
- *The Business / m-Consumer$_j$ / Personal Network*: are parties or entities with which the m-Consumer wishes to communicate. The *business* party corresponds to the collector in the Head & Yuan framework (Head and Yuan 2001). The *m-Consumer$_j$* and *personal network* correspond to the entities identified by the same name in the Coursaris and Hassanein framework for m-Consumer interaction modes within a wireless environment (Coursaris and Hassanein 2002).
- *The Violator*: who corresponds directly with the *violator* described above (Head and Yuan 2001)
- *The Protector*: who corresponds directly with the *protector* described above (Head and 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 which can be collected and passed through wireless communication: (i) ***who*** refers to the identities of the sender and/or receiver; (ii) ***what*** refers to the content being communicated; (iii) ***where*** refers to the location of the m-Consumer; (iv) ***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 that the m-Consumer interacts with. Figure 9 represents the activities of the violator by crooked or jagged arrows. The protector encircles the interactions within 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-Consumer the ability to block some of their personal identity.

Having identified the privacy parties and the types of information exchanged between them within a wireless environment, we can now analyze 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.

5. Discussion

The discussion in section 3 identifies the main ingredients necessary to protect one's right to control the flow of information about themselves over wireless networks. These ingredients are privacy, security, and legislation. It is only upon addressing the issues related to these three areas and with education acting as a catalyst that consumer privacy may be effectively protected. 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. Privacy in m-Commerce extends from the information context to also include a consumer's physical space. As such, the concern is escalated compared to the level of privacy concern for e-Commerce and a consumer needs to be armed with knowledge on their responsibilities, business' information practices, as well as possible courses of action in the event of privacy violation. Unfortunately, a survey of IT Security Professionals in the United States identified the primary obstacle to achieving adequate information security levels as being the lack of end-user awareness (Foran 1996). Thus, the fundamental requirement here is for consumers to learn about privacy and security measures, and adjust security and privacy settings to their satisfaction on their wireless devices. 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 on whether to interact with that business accordingly. 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 setup proper defense systems. Consequently, a business' primary responsibility is to implement security measures to prevent 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 2000). Finally, the issue of industry standards arises, when consumers are stuck 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, a consumer's private information may be used without his or her consent, due to the different network carrier policies. 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-1990's 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 for privacy. The privacy standards set in PIPEDA were derived from the Canadian Standards Association's *Model Code for the Protection of Personal Information* (Canadian Standards Association 2001). This was a joint effort between business, government, and consumers, and as such 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 so far have 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, then 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 similar privacy policies 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 gray 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.

6. 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 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 presented in Section 4 of this paper. This matrix 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 slow down in e-Commerce success. Privacy, security, and legislation combined with education can facilitate strong privacy protection practices, maintaining the consumer's interest in mind 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 within 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 within any industry. However, this framework should be scrutinized, and potentially modified, within 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, Bodler than You Imagine”, 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”, http://www.acnielsen.com/news/american/ca/2000/20000127.htm.

Agranoff, M. H. (1993). "Controlling the Threat to Personal Privacy." *Journal of Information Systems Management*, Summer.

Allison, C., J. Moss, et al. (2001). "Wireless Location Technologies: Options for E-911 and Beyond." The Strategis Groups http://www.wow-com.com/market_research/documents/1270-01_ExSum.pdf.

Bask, J. (2001). "Pervasive Computing: Travel and Business Services." Telecommunications Software and Multimedia Laboratory http://www.tml.hut.fi/Studies/Tik-111.590/2001s/papers/joni_bask.pdf.

Cam, N., J. Walker, et al. (2001). "Rapid Re-Keying WEP a recommended practice to improve WLAN security." IEEE http://www.drizzle.com/~aboba/IEEE/.

Camp, L. J. (1999). "Web Security and Privacy: An American Perspective." *The Information Society: An International Journal*, 15(4): pp. 249-256.

Canadian Standards Association (2001). “*Model Code for the Protection of Personal Information.”*, http://www.csa.ca/standards/privacy/default.asp?load=code&language=English

Canadian Wireless Telecommunications Association (CWTA) (2002). "Wireless Facts and Figures." http://www.cwta.ca/industry_guide/facts.php3.

Cavoukian, A. and M. Gurski (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*: http://www.internetworld.co.uk/mcomm/vRoot/articles/article.cfm/B6D4ACE6-D1D4-11D4-BEE900B0D0A143DF.

Coursaris, C. and K. Hassanein (2002). "A Framework for m-Commerce: A Consumer's Perspective". *3rd World Congress on the Management of Electronic Commerce*, Hamilton, Ontario, Canada.

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

European Commission (1999). "Directive 95/46/EC of the European Parliament." http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

Fisher, D. (2001). "WLAN Security in Neutral." *eWeek*: http://www.eweek.com/article/0,3658,s%253D701%2526a%253D20541,00.asp.

Foran, B., (1996). “Censorship and Privacy Issues for Law Enforcement”. The 91st Annual Canadian Association of Chiefs Of Police Conference. http://privcom.gc.ca/speech/archive/02_05_a_960826_e.asp

Gururajan, R. (2002). "Mobile Computing: Security Risks". *23rd World Congress on the Management of Electronic Commerce*, Hamilton, Ontario, Canada.

Head, M. M. and Hassanein, K. (2002). “Trust in e-Commerce: Evaluating the Impact of Third-Party Seals.” *Quarterly Journal of Electronic Commerce (2002)* (to appear).

Head, M. M. and Y. Yuan (2001). "Privacy Protection in Electronic Commerce: A Theoretical Framework." *Human Systems Management*, 20: 149-160.

Ipsos-Reid (2001). "The Face of the Web." http://www.ipsos-reid.com/media/dsp_displaypr_cdn.cfm?id_to_view=1229.

Johnson, D. (2002). "Securing your PDA." IDG.net http://www.idg.net/ic_794581_5056_1-2887.html.

Keyte, C. (2001), "It's not about the phones!", m-Commerce World, http://www.internetworld.co.uk/mcomm/vRoot/articles/article.cfm/A0154418-21C5-11D5-A04E00C04FA0E16A.

Koster, E. H. (1999). "Zero Knowledge: Personal Data on the Internet." *The Computer Lawyer* May: http://www.oppenheimer.com/intprop/news/zeroprivacy.shtml#worth.

Leiner, B. M., Cerf, Vinton G., Clark, David D., Kahn, Robert E., Kleinrock, Leonard, Lynch, Daniel C., Postel, Jon, Roberts, Larry G., Wolff, Stephen (2002). "A Brief History of the Internet." Internet Society http://www.isoc.org/internet/history/brief.shtml.

Little, J. (2001). "M-Commerce." *imazing!CJRW*: http://www.cjrw.com/imazing/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*: http://www.zdnet.com/intweek/stories/news/0,4164,2445298,00.html.

Middleton, J. (2001). "Lost Mobile Devices drive security fears." *vnunet.com*: http://www.vnunet.com/News/1125076.

Morrison, D. (2001). "Technology Push and Customer Pull: The Wireless Internet Comes of Age." Presentation at McMaster University.

NCR Corporation, 2003 "Teradata Personal Data Protection Principles" http://www.teradata.com/main/privacy.asp.

Nielsen, J. (2000). *Designing Web Usability: The Practice of Simplicity*. Indianapolis, Indiana, New Riders Publishing.

Peck, A. (2001), *WAP's summer of discontent*, m-Commerce World, http://www.internetworld.co.uk/mcomm/vRoot/articles/article.cfm/87DB2C1B-D4FC-11D4-A9E300C04FA0E16A.

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

Pocket Directory (2001), "Smart Phones", http://www.pocketdirectory.com/hardware/hproducts.aspx?idCat=4&selHId=1.

Privacy Commissioner of Canada (2000). "Statutes of Canada 2000." *Website:* http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp.

Privacy Commissioner of Canada, 2002, *"Privacy Legislation in Canada 2002"*, http://www.privcom.gc.ca/fs-fi/fs2001-02_e.asp.

Rainio, A. (2001). "Location-Based Services and Personal Navigation in Mobile Information Society". *New Technology For A New Century - Technical Conference*, Seoul, Korea http://www.ddl.org/figtree/pub/proceedings/korea/full-papers/pdf/plenary1/rainio.pdf.

Reid, Hon. John M. (2001). "REMARKS TO SECURITY & PRIVACY for GOVERNMENT ON-LINE CONFERENCE". http://infocom.gc.ca/speeches/speechview-e.asp?intspeechId=5

Rogers Communications (2002). "Network Coverage Info". Rogers website. http://www.shoprogers.com/store/wireless/coverage/overview.asp?shopperID=8SXT109NSKS92JE200J74HJFP4PK5ME0.

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

Statistics Canada (StatCan) (2001). "The 2000 Household Internet Use Survey." http://www.statcan.ca/Daily/English/010726/d010726a.htm.

UCLA Center For Communication Policy (2001). "The UCLA Internet Report 2001: Surveying the Digital Future."

Table 1: Comparing Canada and US adoption rates for various technologies

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

Table 2: Characteristics of m-Commerce Consumer Business Applications
(Adapted from: Coursaris-Hassanein 2002)

Business Application	Needs °				Interaction Modes✦	Concerns
	1	2	3	4		
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^2	Cost
Information						
- Web browsing	√	√	√	√	W_{B2C}	Cost, Usability
- Traffic/Weather		√			W_{B2C}	Privacy, Usability
Entertainment						
- Gaming			√	√	W_{B2C} W_{C2C}	Cost, Usability
- News/Sports		√	√	√	W_{B2C}	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. Communication, 2. Information, 3. Entertainment, 4. Commerce

✦ W_{B2C}: Wireless Business to Consumer Interaction, W_{C2C}: Wireless Consumer to Consumer Interaction, W_C^2: Wireless Consumer to self Interaction (e.g. with personal home network)

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$_j$'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

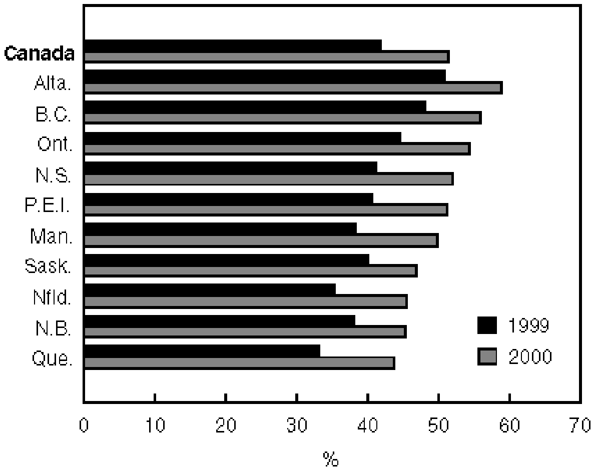


Figure 1: Canadian Internet penetration rates, for different provinces (Statistics Canada 2001).

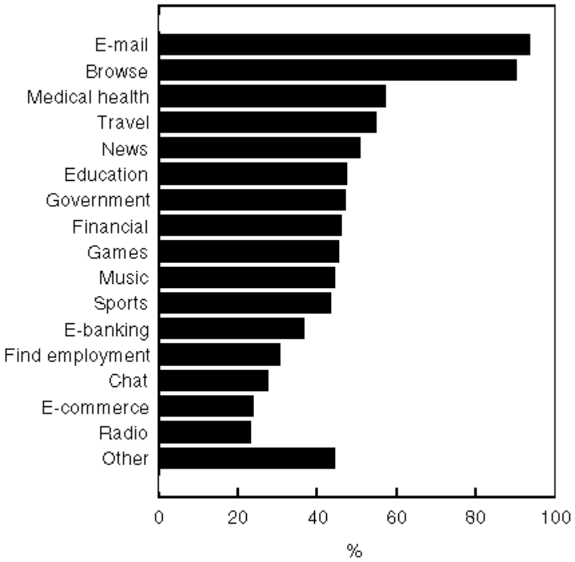


Figure 2: Internet applications frequently accessed by regular Canadian users from home, 2000 (Statistics Canada 2001)

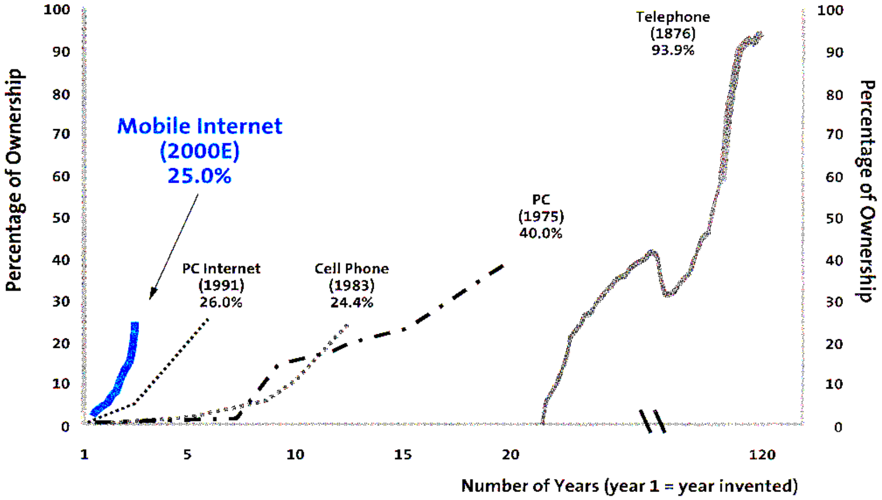


Figure 3: U.S. adoption rates for various communication and Internet access devices (Morrison 2001)

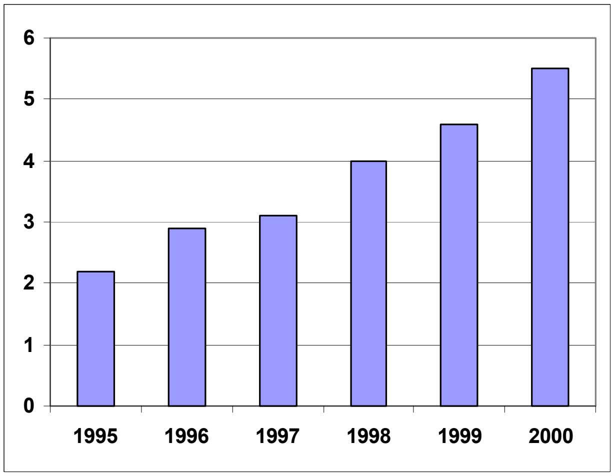


Figure 4: Canadian Cellular/PCS Revenue in $Billions
(Canadian Wireless Telecommunications Association 2002)

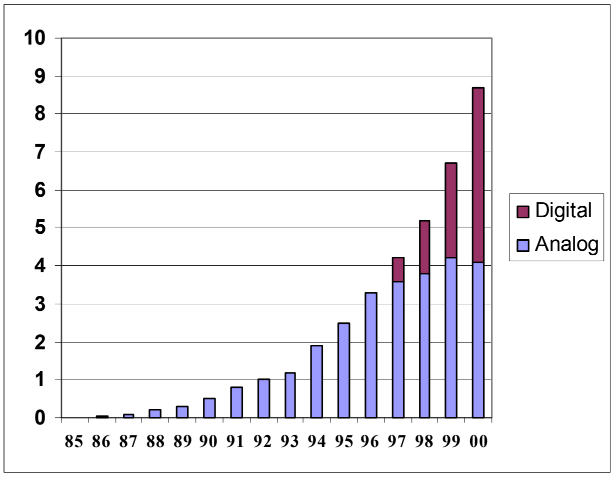


Figure 5: Canadian Cellular/PCS Growth in Millions subscribers
(Canadian Wireless Telecommunications Association 2002)

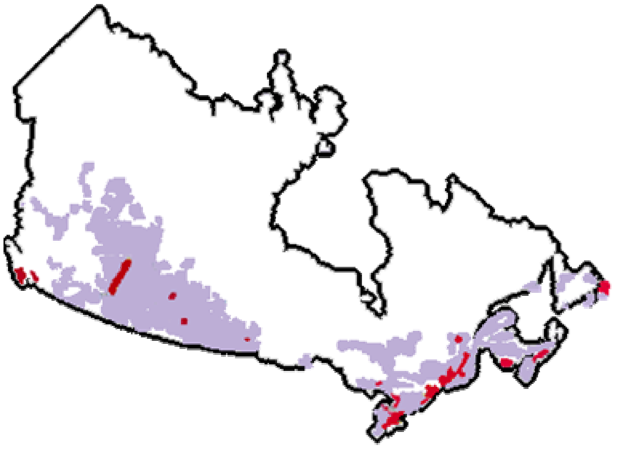


Figure 6a: Bell Mobility Wireless Network

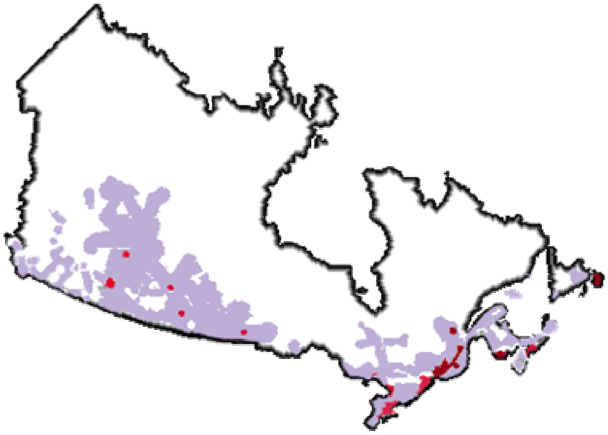


Figure 6b: Rogers AT&T Wireless Network

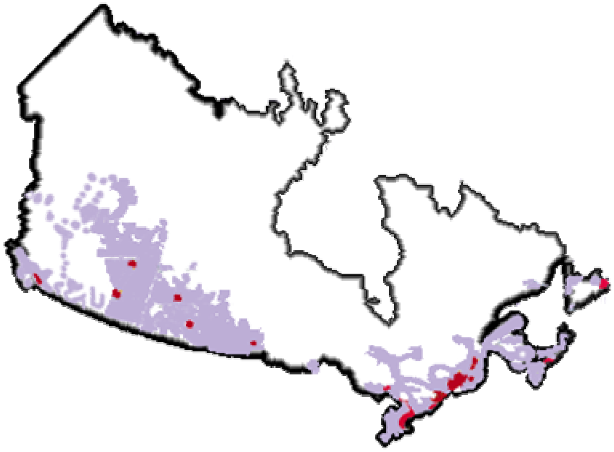


Figure 6c: Telus Mobility Wireless Network

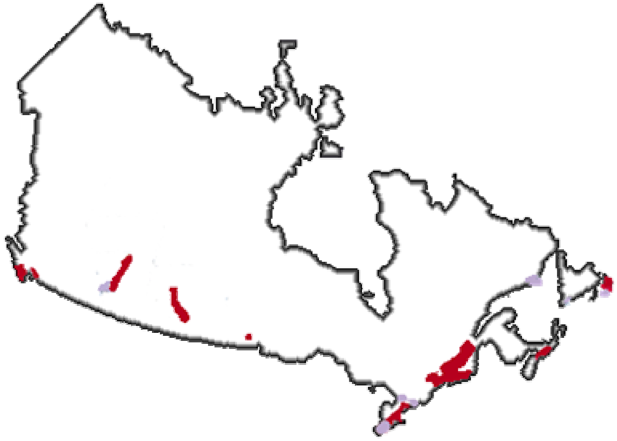


Figure 6d: Microcell (Fido) Wireless Network

Key: 🟪 Analog coverage 🟥 Digital coverage

Figure 6: Wireless Networks in Canada

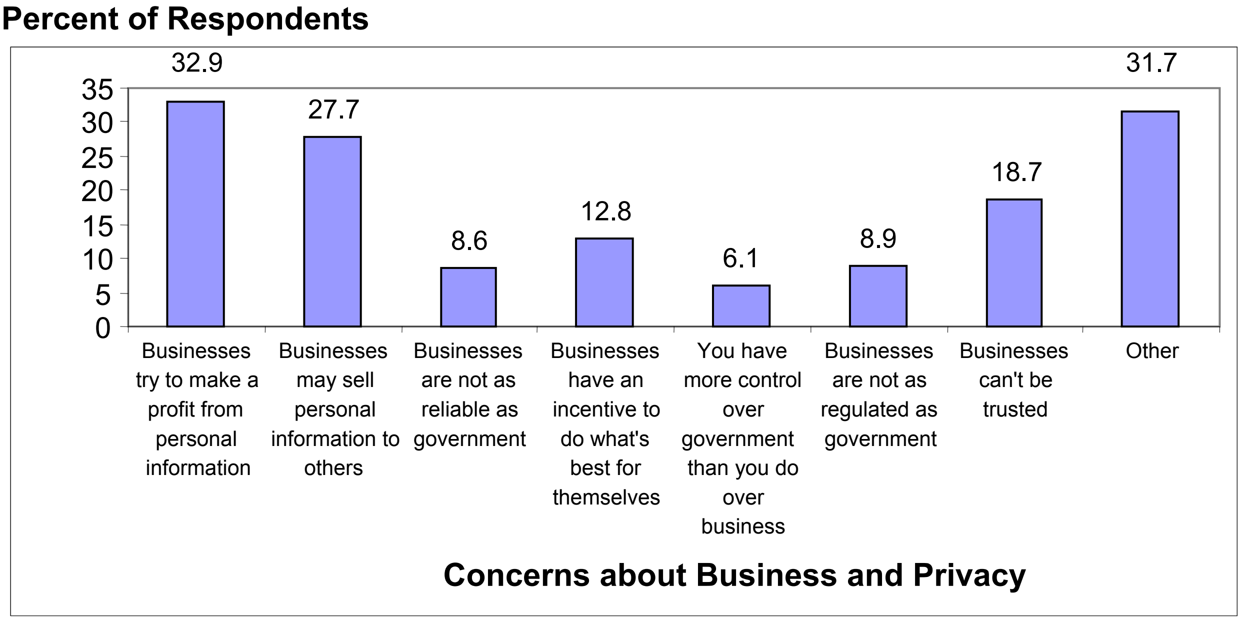


Figure 7: Reasons cited for privacy concerns in dealing with businesses online (UCLA Center for Communication Policy 2001)

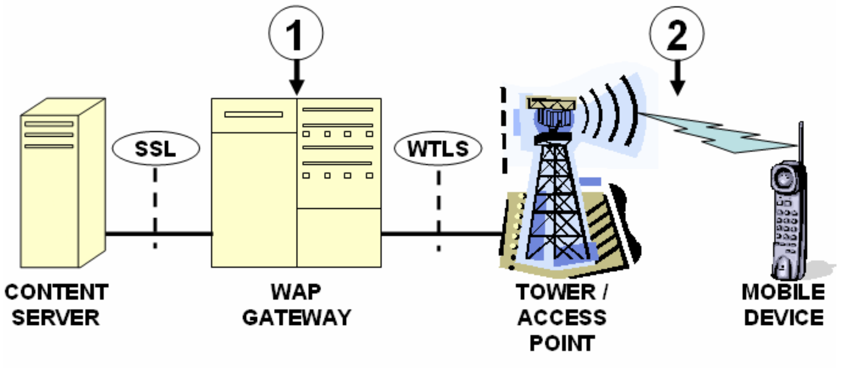
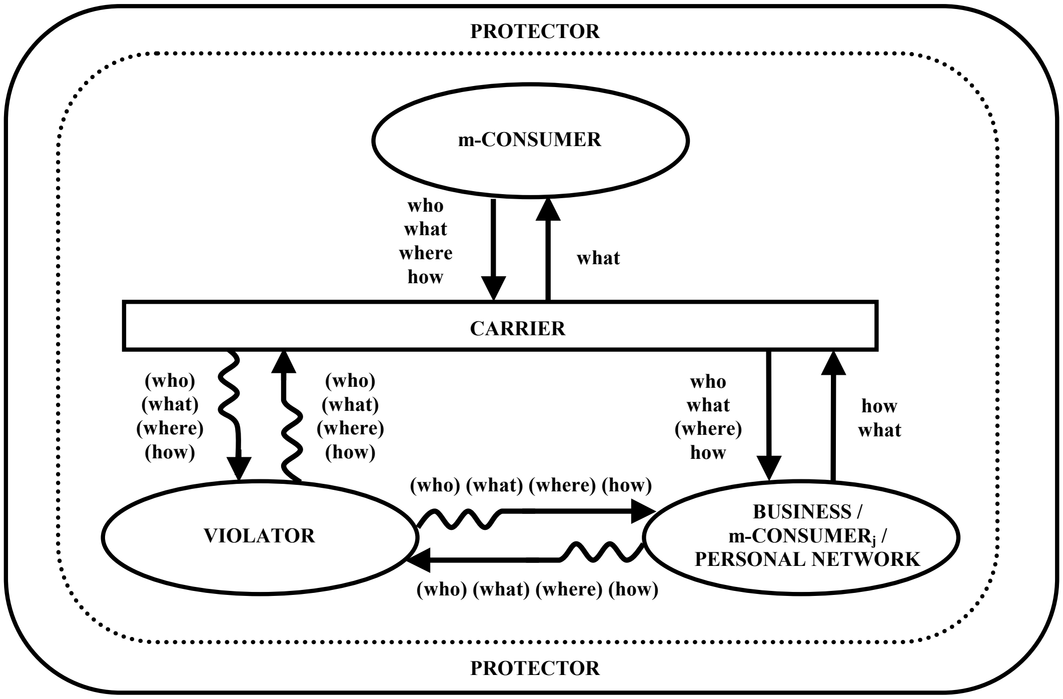


Figure 8: Required infrastructure for WAP wireless telecommunication



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

Figure 9: Wireless Privacy Interaction Framework