



Prepaid Mobile Phone Service and the Anonymous Caller: Considering Wireless E9-1-1 in Canada.*

Gordon A. Gow¹ and Mark Ihnat²

Abstract

This paper reports on a recently concluded empirical study into the development of Wireless E9-1-1 (emergency service) in Canada that initially focussed on privacy concerns raised in the context of an emerging location based service (LBS) for mobile phone users. In light of existing regulatory arrangements this paper concludes that in Canada the emerging Wireless E9-1-1 system establishes a reasonable level of protection for the privacy rights of mobile phone users who choose to contact emergency services. However, an important and surprising issue was raised in the proceedings regarding the obligation of wireless service providers offering prepaid mobile phone service to obtain verifiable subscriber records from their customers. This paper provides details regarding the issue and contributes a number of points to an emerging debate concerning the right to anonymity for customers who elect to use prepaid or other services provided over commercial networks.

Introduction

Within the past decade or so, the dissemination of wireless communication devices has resulted in a dramatic loading on public safety agencies to the extent that, as a percentage of total emergency (9-1-1) service calls, mobile phones will soon represent over fifty per cent.³ A significant problem for 9-1-1 operators when dealing with calls placed from mobile phones is identifying the location of a caller in distress, as these callers are often unable to report a specific location and thus create problems for determining appropriate assignment of emergency dispatch and response. Wireless enhanced emergency service ('Wireless E9-1-1') is a new service innovation being introduced into the public telephone network across North America that

* This research was funded in part with grants from the Social Sciences and Humanities Research Council of Canada (SSHRC) and Canada's Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP).

¹ Department of Media and Communications, London School of Economics and Political Science, UK.
<mailto:g.gow@lse.ac.uk> or <mailto:gagow@sfu.ca>

² School of Communication, Simon Fraser University, Canada.

³ This claim is based on personal communications with a representative of the public safety answering point in the Greater Vancouver Regional District.

provides the location information of a mobile phone caller to a 9-1-1 operator. It promises to assist in emergency services dispatch and to dramatically enhance public safety through improved response times. Its development in Canada has also raised concerns about customer privacy rights and the collection of personal information when purchasing prepaid mobile phone service.

This paper reports on a recently concluded empirical study into the development of Wireless E9-1-1 in Canada. The study itself examined numerous aspects of the regulatory and industry processes involved in creating this early form of location-based service. The research was informed by published studies in the dynamics of large technical systems and drew upon methods developed within the field of constructivist technology studies supported by extensive analysis of source documents filed with the Canadian Radio-television and Telecommunications Commission (CRTC) and the Canadian Wireless Telecommunications Association (CWTA). Findings from the study indicate that the emerging Wireless E9-1-1 system establishes a reasonable level of protection for the privacy rights of mobile phone customers who choose to contact emergency services. However, an important and surprising issue was raised during the proceedings regarding the obligation of wireless carriers to collect and disclose personal information from their prepaid customers. This paper explores this issue as it was manifested in the Wireless E9-1-1 case, suggesting that the matter coincides with a wider debate concerning the regulation of electronic networks and the right of users to remain anonymous while using these technologies.

The Genesis of Wireless E9-1-1

The story of Wireless E9-1-1 begins in the United States, with the Federal Communications Commission's (FCC) *Notice of Proposed Rule-Making* under Docket 94-102, issued in October of 1994. The primary intent of this Notice was to launch a series of related initiatives to improve public safety in light of the growing concern over the impact of mobile phones at the public safety answering points (PSAPs). Over the course of some thirty-five years, public safety groups across the U.S. had developed a rather advanced system for providing telephone access to PSAPs for requesting emergency services (National Emergency Number Association, 2002a). The first stage in this history was the informal adoption of a simple, widely known number that people could easily remember to call during an emergency. The digits 9-1-1 were eventually selected for this purpose. Among other things, the Notice proposed to formalize 9-1-1 as the nation-wide number for placing emergency calls.

The original 9-1-1 system was designed as a simple voice connection to an operator designated to handle emergency calls and dispatch appropriate agencies as required. With the subsequent development of more sophisticated telecommunications services, an enhanced 9-1-1 system was implemented whereby the voice path connection was augmented with two data elements: the telephone number from which the call is being made and the street address associated with the telephone number (National Emergency Number Association, 2002b). With these two pieces of information, an emergency operator now had more information available to improve dispatch operations. With automatic telephone number identification (ANI) calls could be returned in the

event they were disconnected, or the number could be provided to law enforcement agencies to support follow-up investigations. Furthermore, the ANI could be crossed reference with an automatic location identification (ALI) database to provide the emergency operator with the street address associated with the telephone number. Emergency calls could be now more easily re-directed to appropriate jurisdictions for dispatch and, in the event a caller was unable to provide their location verbally to the operator, emergency personnel could be directed to the exact spot from which the call had originated. This ANI/ALI (pronounced ‘Annie-Alley’) functionality has since become the benchmark feature of E9-1-1 across North America.

With the rapid uptake of mobile phones beginning in the mid-1990s, the well-established E9-1-1 system was quickly becoming fragmented into wireline calls with ANI/ALI functionality and calls from mobile phones that offered no enhanced functionality whatsoever. This was because the original E9-1-1 service had been conceived within a wireline environment in which telephone numbers were more or less permanently associated with street addresses. Mobile phones undermine this design, as a mobile phone number is not necessarily associated with a fixed physical location. Moreover, the typical interconnection arrangements between wireless carriers, incumbent carriers, and the public safety answering points made it technically impossible to provide the enhanced functionality for mobile phones. This meant that emergency operators were not even receiving a telephone number from the wireless calls, leading to delays in dispatching emergency personnel. A new system for E9-1-1 would need to be developed to enable the ANI function in addition to some form of *dynamic assignment of location information* for mobile phones.

The FCC was determined to solve the problem of Wireless E9-1-1 by establishing a two-phase process by which wireless carriers would be required to provide ANI/ALI information to local public safety answering points (PSAPs). In the first phase of the process the U.S. wireless carriers were required to provide a system that would provide a local PSAP with the ANI of a mobile caller plus low-resolution location information in the form of cell-site or cell-sector address from which the call had been placed to 9-1-1. The second phase requirements are more rigorous and demand that the wireless carriers implement a system that provides ANI plus *high-resolution* location information in the form of near real-time latitude/longitude coordinates of the mobile phone. High-resolution is defined according to the system that a carrier chooses to implement. For handset-based solutions the FCC has set an accuracy/reliability requirement of 50 metres for 67 percent of calls and 150 metres for 95 percent of calls. For network-based solutions, the FCC requires an accuracy of 100 metres in 67 percent of calls and 300 metres for 95 percent of calls.⁴ Phase 1 deployment was originally set at April 1998 and Phase 2 at October 2001. The FCC has since revised the Phase 2 deployment timeline, commissioned a major investigation, and created a wireless ‘outreach’ program in the wake of many U.S.

⁴ A typical handset-based solution uses GPS (Geographic Positioning System) that involves placing a small receiver in the mobile phone to enable it to report its physical location using satellite-based radio signals. Network-based solutions, by contrast, use triangulation techniques calculated at cellular base stations or control points in the wireless network. An advantage of the network-based solution is that mobile phones need not be modified with GPS in order to be located in geographical space. The website of the Alabama chapter of the National Emergency Number Association (NENA) offers a good explanation of these solutions: http://www.al911.org/wireless_home.htm

carriers failing to meet the original deadline (Federal Communications Commission, 2001, 2003).

FCC Phase	Requirement
0	Transmit all 9-1-1 calls to a PSAP
1	Transmit ANI and cell-site/sector
2	Transmit ANI and lat/long location

Table 1: *FCC Wireless E9-1-1 Requirements*

For many of those in the U.S. wireless industry, the FCC regulatory initiative inaugurated what was believed would be a rush by industry to deploy a suite of commercial location-based services to recover the cost of deploying Wireless E9-1-1. Numerous location-tracking vendors appeared in conjunction with the FCC mandate and the Wireless Location Industry Association was formed as an industry body to promote location based services (Wireless Location Industry Association, 2001). Speculation in the trade press and much of the popular media also reflected an optimistic sense of inevitability with respect to the future of mobile positioning and location based services.

Privacy Concerns with respect to Wireless E9-1-1

It is important to note that the initial E9-1-1 development for wireline telephone service was undertaken within the monopoly telecom regimes of both the U.S. and Canada prior to the AT&T divestiture in the early 1980s. As such the deployment of this enhanced functionality occurred gradually throughout North America and under very tightly regulated conditions that placed clearly defined limits on the disclosure of customer information. There is little apparent evidence to suggest that it raised significant privacy concerns with the press or among the general public. Yet, the prospect of tracking the location and movement of mobile phones within a post-divestiture competitive telecom sector almost immediately grabbed the attention of those concerned with privacy rights and with the prospect of unwanted government and corporate surveillance that might be made possible using this new technology.

In addition to fairly extensive coverage of this issue in the popular press, a small number of studies have also been made available on privacy rights and unwanted surveillance under the FCC wireless mandate. David Phillips, for instance, has suggested that the Wireless E9-1-1 initiative “has created the infrastructure for a general purpose locational surveillance system capable of identifying, tracking and responding to individuals” (Phillips, 2003). According to Phillips, this is an implication of the design of the Wireless E9-1-1 system, especially if we consider the potential of Phase 2 systems to track the movement of mobile phone customers with high degree of accuracy, allowing for a rather extensive surveillance matrix that facilitates “institutional practices of tracking and locating individuals, profiling individuals, rationalizing space, creating places, and encouraging appropriate actions in appropriate places.” Whereas the original E9-1-1 provided possibilities for simple wiretapping and call tracing of the individual while at home or in the office, Phillips believes that wireless E9-1-1 when combined with the recent introduction of other law enforcement and national security legislation has extended these

possibilities to enable pervasive surveillance or at least the possibility of such no matter where the individual is located.

A related study conducted into privacy implications for Wireless E9-1-1 in the United States and Canada concluded with two primary concerns: the first being that “wireless E9-1-1 has produced an environment “that is less sensitive to the privacy concerns of individuals and more attuned to surveillance of populations...”; the second being that this environment engenders a design, or what the authors term an “architecture”, for Wireless E9-1-1 that will dictate future privacy possibilities. In other words, if privacy rights do not take centre stage in the planning of this location based service, the authors of this study argue that “its protection will never be as secure as it needs to be” (Regan, Bennett, & Phillips, 2002: 25).

Such an infrastructure for surveillance need not only serve law enforcement or government agencies. Aaron Futch and Christine Soares (Futch & Soares, 2001) argue that without “clear privacy policies in place, retailers and specialty advertising and marketing companies are gearing up to take advantage of location information” generated by the emerging technology that will enable location tracking of some 120-million wireless customers in the United States.⁵ The value of Wireless E9-1-1 as a public safety measure is not being questioned; rather, here the concern is being raised with the disclosure of mobile phone location information to third parties such as marketing firms or local businesses wanting to capitalize on its potential for attracting nearby customers.

Generally speaking, concern about privacy and surveillance with Wireless E9-1-1 centres on the disclosure of information related to the location of mobile phones operating on a wireless carrier’s network. Related to this concern is another issue of customer consent over this disclosure, as well as the terms and conditions on which a mobile phone customer may choose to *deny* access to personal information including their location. Bennett, for example, points out quite rightly that part of the attraction of using one’s mobile phone for emergency calls is the ‘anonymous Good Samaritan’ factor where identity of a mobile caller is not revealed (Bennett & Regan, 2002). However, as we shall detail in a moment, the transmission of a caller’s mobile phone number (ANI) and their real-time location (ALI) does not necessarily prevent callers from remaining anonymous.

The issue of customer consent is addressed to some extent in American legislation passed following the launch of the FCC mandate to create nationwide Wireless E9-1-1 capability. The *Wireless Communications and Public Safety Act* was passed in 1999 and amends section 222 of the Telecommunications Act of 1996 to authorize the provision of “call location information concerning the user of a commercial mobile phone service” solely for the purpose of responding to an emergency situation. This authorization restricts disclosure to emergency response situations unless “express prior authorization of the customer” has been provided to use it for other purposes. Likewise, a wireless carrier is required to disclose all subscriber list information that “is in its possession or control” including information pertaining to subscribers

⁵ There are currently more than ten million wireless customers in Canada according to the Canadian Wireless Telecommunications Association.

whose have chosen to be ‘unlisted’ in a public directory. Bennett and Regan have noted that these amendments to the legislation seem on the one hand to require that customers actively ‘opt-in’ to secondary uses of call location information that are unrelated to emergency response. On the other hand, however, they have observed that

More generally the [legislation] appears to categorize location information as customer proprietary network information (CPNI) which cannot be disclosed to third parties without a customer’s consent or statutory exception. The location information that wireless carriers [might choose to] collect for non-emergency purposes would appear to be thus classified as CPNI. The courts, however, have ruled that telecommunications companies cannot be required to have customer’s “opt-in” to uses of CPNI. The standard then for location information gained through non-emergency reasons would be “opt-out.” (Bennett & Regan, 2002)

In other words, the decision by US lawmakers to categorize location information as customer proprietary information (CPNI) has important implications for customer consent over the use of that information. If location information is classified as CPNI, then it appears as if it is subject to ‘opt-out’ provisions under current American law, which means that wireless service providers can elect to disclose such information for non-emergency reasons unless their customers actively choose to decline it. More generally, CPNI has been at the centre of longstanding debate over the privacy rights of telephone subscribers in the United States driven in part by telephone companies who claim that this is information falls within the domain of commercial speech rights (Sparks, 2000).

The definition of CPNI was modified by the *Wireless Communications and Public Safety Act* (WCPS Act) to include location information and now reads as follows:

[CPNI is defined as] information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, *and that is made available to the carrier solely by virtue of the carrier-customer relationship.* [emphasis added]

(Legal Information Institute, 1999)

Essentially, CPNI is that body of data generated within a telecommunications network for the purpose of customer billing: what numbers were dialed, the type of call (e.g.: a long distance collect call), the duration of the call, the general location of the callers (necessary when invoicing mobile subscribers who have roamed outside their home region). The location element is now modified and given greater precision with the advent of Wireless E9-1-1. Section 222 of the WCPS Act identifies three forms of customer information, subject to a graduated level of protection:

- Subscriber list information (name, address, and telephone number)
- Anonymous CPNI (network activity traceable to a telephone number only)
- Identifiable CPNI (network activity traced to a telephone number and associated with subscriber list information)

Subscriber list information is collected for the publishing of directories and service providers do not require customer approval to disclose it for such purposes. Anonymous CPNI can also be disclosed without customer notice. Identifiable CPNI, however, cannot be disclosed without prior approval of the identified individual customer (Sparks, 2000: 6).

It is important to note that subscriber list information must be combined with anonymous CPNI to produce an individual customer profile. In most cases a telephone service provider must take steps to do this for the purpose of billing, using the telephone number as a common referent. And, as noted above, under the new wireless legislation telephone service providers are required to disclose subscriber list information during emergency response situations whether or not it is associated with CPNI. This is in part because the useful value of CPNI to emergency responders and other potential interested parties is derived only when it is associated with the name and address associated with the telephone number. Stripped of such an association, CPNI by itself is simply a data profile not inherently traceable to any particular individual.

This observation may have implications for the collection of personal information by wireless carriers and PSAPs when establishing a Wireless E9-1-1 service and speaks to aforementioned concerns about privacy rights and the emerging architecture of this system. According to its definition in current American legislation it appears as if the raw form of CPNI is perfectly suited to meet the FCC's functional requirements because, unto itself, it fulfills the ANI/ALI criteria. Current legislation notwithstanding, there is no apparent need to associate the telephone number and location with any personal information, such as name or home address, for a caller who has dialled 9-1-1 from a mobile phone. A caller could choose to disclose such information voluntarily if so requested by the emergency operator without affecting the essential functional performance of the Wireless E9-1-1 service as currently defined by FCC mandate.

Perhaps the most apparent challenge to the collection of personal information in the carrier-customer relationship is with prepaid mobile phone services, where there is no operational requirement to cross-reference with CPNI with subscriber list information for billing purposes. In a prepaid arrangement a mobile telephone number is 'charged up' using a prepaid calling card that can be purchased anonymously. As the customer uses the phone service, CPNI is generated and used to keep track of the prepaid account balance. When a customer's account is depleted, a new calling card is purchased and the mobile phone is again charged up. In other words, in a prepaid service arrangement CPNI is tracked to the mobile telephone number and not to the customer *per se*. While some wireless carriers may have a policy of collecting customer personal information upon activation of a prepaid mobile phone account there is no inherent reason for this information to be associated with any CPNI generated through the use of that prepaid service.

This point raises two matters for consideration: first, it questions the legitimacy of collecting personal information for prepaid telephone service and, second, it suggests an expanded discourse within which to consider privacy concerns related to Wireless E9-1-1, as it falls within the fold of a wider debate about setting limits on the disclosure of personal information held by a telephone service provider and used in conjunction with the collection of CPNI. In this respect Wireless E9-1-1 is not as unique a development as one might think at first encounter, as the

CPNI debate has a fairly extensive history and background that scholars and privacy advocates may draw upon (Electronic Privacy Information Centre, 2003).

The issue of prepaid services, however, opens a new set of questions around the right of customers to expect a reasonable degree of anonymity when using such a service. Consolidated statistics for the US market are harder to obtain but Canadian figures give an indication of the North American sector and reveal that prepaid services account for about 30 percent of total mobile phone subscribers, while in certain segments of the market it now surpasses 50 percent (Canadian Wireless Telecommunications Association, 2003), suggesting a significant shift away from the traditional customer-carrier relationship to new forms of service provision for telecommunications. In the United States, the FCC recently clarified that prepaid services and the related phenomenon of disposable mobile phones do fall under the E9-1-1 mandate but it is yet unclear as to how the American regulator will decide to deal with collection of personal information for these services (Hanson, 2003).⁶

Background to Wireless E9-1-1 in Canada

The issue of privacy in the Canadian context with regards to Wireless E9-1-1 has so far been a peripheral concern within regulatory proceedings. Privacy concerns have sparked little public debate in Canada, which is a departure from the American approach where the “the issue of locational privacy is firmly on the political agenda” with respect to the ANI/ALI technology (Bennett & Regan, 2002). Rather, a concern with technical trials, the regulator’s demands for ad hoc interim solutions, and growing volatility in the relationship between wireless service providers (WSPs) and public safety answering points (PSAPs) have so far dominated the proceedings on Wireless E9-1-1 in Canada (Gow, 2002).

As it stands, current commercial practice and regulatory requirements in Canada limit the disclosure of customer information when calls are dialed to 9-1-1. Commercial agreements between Wireless Service Providers and the 9-1-1 network operator (usually the incumbent wireline carrier) have strict provisions for data record confidentiality as directed by the CRTC (Bell Canada, 2000). The CRTC ruling is stated in Decision 99-17 and makes reference to general provisions for 9-1-1 service and standard agreements between carriers and municipalities providing 9-1-1 services at Public Safety Answering Points (PSAPs). Under these standard agreements, confidential customer information is provided on “a call-by-call basis solely for the purpose of responding to emergency calls”. However, the agreement that defines the terms of service for end-users states that the customer “waives the right to privacy to the extent that the confidential information in the ALI database is provided to the PSAP” (Canadian Radio-television and Telecommunications Commission, 1999). These arrangements limit, in a similar way to the American legislation, the use to which customer information can be used when provided during an emergency call to 9-1-1 but also as in the American case permits the

⁶ A related problem is that of ‘uninitialized’ mobile phones. These are phones not registered for service with any commercial mobile carrier and include special “911-only” devices. The wireless industry in Canada and the United States has agreed to accept 9-1-1 dialled calls from uninitialized phones, creating a challenge for tracing these calls (Federal Communications Commission, 2002).

disclosure of *any and all information* that may be present within the system at the time of the call, including subscriber list information associated with anonymous CPNI.

The Canadian situation differs slightly from the American insofar as Canada has introduced the *Personal Information Protection and Electronic Documents Act* (PIPED Act), in an attempt to “establish rules for the management of personal information by organizations involved in commercial activities” (Privacy Commissioner of Canada). The application of the Act currently applies to all federally regulated commercial organizations, including telecommunications service providers. The PIPED Act is based on the CSA Model Code for the Protection of Personal Information and modeled on a set of fair information principles established by international data protection standards. The Act marks a major step towards reaffirming privacy rights in Canada as it applies to the collection, use and disclosure of the personal information of employees and customers of telecommunications service providers. Individuals are now given the legal power to question the purpose of collecting certain information and question how such information will be used and disclosed. Furthermore, the PIPED Act establishes a mandatory consent option, which must be offered to an employee or customer stating that consent must be given for the collection and disclosure of personal information. In the case of providing 9-1-1 service this consent is granted within the customer-carrier relationship as regulated by the CRTC (described previously).

Section 5 of the PIPED Act establishes general terms and conditions for the protection of personal information in Canada. Contextual factors are fundamental to such terms and conditions as stated in section 5.3, “An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances” (Privacy Commissioner of Canada, 2000). In other words, the collection, use or disclosure of subscriber list information in conjunction with CPNI is subject to a test of reasonable appropriateness. On the one hand, such activities might be lawful under the terms of service between a telephone service provider and its customers, and indeed in a number of cases the Privacy Commissioner of Canada has found this to be the case (Privacy Commissioner of Canada, 2003). On the other hand, however, section 5.3 might be used to call into question the reasonable appropriateness of collecting subscriber list information for prepaid mobile phone customers. Moreover, given that anonymous CPNI provides enough information alone to meet the FCC Wireless E9-1-1 standard, it is conceivable that mobile phone customers who subscribe to monthly billing plans might also choose to assert a right of consent over the disclosure of personal details for emergency response, although such a scenario has yet to be put before the Privacy Commissioner.

Ongoing deliberations over the design of Wireless E9-1-1, and more specifically the ALI database structure, may play a significant role in determining what is deemed reasonable and appropriate in terms of collection of personal information for prepaid mobile phone services. As we hope to illustrate in the next section, minor modifications to the design of the existing ALI database, as determined in regulatory proceedings or through industry voluntary efforts, may have far reaching consequences for the protection of personal privacy rights in Canada vis-à-vis current federal legislation.

We have attempted to show so far that the functional requirements of Wireless E9-1-1, as defined by the FCC mandate, do not require the association of anonymous CPNI with subscriber list information. This is most evident in the case of prepaid mobile service, but there appears to be no reason why it need not be a principle applicable to other mobile telecommunications services. Indeed, with pay telephones it is currently the case that E9-1-1 is served while retaining the anonymity of the caller. Highlighting and preserving this functional distinction may be an important consideration in future debates about the design of Wireless E9-1-1 and other location-based services. This distinction, after all, may be the variable that establishes what is considered reasonable and appropriate information in the customer-carrier relationship for the provision of telecommunications services. In the next section we hope to illustrate this point using a debate that in fact occurred over this very issue during the period that Wireless E9-1-1 was being developed and deployed across Canada.

Tracking the Development of Wireless E9-1-1 in Canada

While the FCC in the United States had initiated an ambitious regulatory effort to promote Wireless E9-1-1, a similar strategy was not being contemplated in Canadian context. Prior to 2000, the Canadian Radio-television and Telecommunications Commission (CRTC) had not taken a position on Wireless E9-1-1 except insofar as it stipulated in its Local Competition Framework that an enhanced 9-1-1 obligation would apply to those service providers wishing to become regulated Competitive Local Exchange Carriers (CLECs). More specifically, paragraph 286 of the local competition framework states the following:

... with regard to 9-1-1 service, all [regulated] service providers must ensure, to the extent technically feasible, that the *appropriate end-user information* is provided to the Automatic Location Identification database to the same extent as that provided by the [incumbent carrier]. [emphasis added]

(Canadian Radio-television and Telecommunications Commission, 1997)

Most mobile phone carriers, also termed Wireless Service Providers (WSPs), are not included in this category and thus not obligated to offer any form of E9-1-1.⁷ If a typical WSP applies to become a fully regulated service provider (a “Wireless CLEC”), however, it must meet the E9-1-1 obligation set out in paragraph 286 of the regulatory framework. Because Canada’s local competition framework is established on principles of technology neutrality and regulatory symmetry, the fact that a carrier provides mobile services is not acceptable grounds for holding the E9-1-1 obligation in abeyance. In fact, the framework was established with the very intention of assuming wireless carriers within its scope of its applicability should they decide to become Wireless CLECs.⁸

⁷ The Canadian regulator is required by legislation to forebear from regulating services that are deemed to reside within a competitive marketplace. Wireless Service Providers fall into this category and are subject to very little regulatory oversight. Emergency number service is a voluntary offering on behalf of the Canadian wireless industry.

⁸ The wording of the paragraph suggests that the authors of the framework may have had in mind *fixed* wireless services as contrasted with *mobile* wireless services.

In view of the fact that the CRTC had decided to forebear from regulating basic mobile phone service (Canadian Radio-television and Telecommunications Commission, 1996) and that there were no Wireless CLECs in Canada at the time, the initiative to develop Wireless E9-1-1 in Canada was therefore left up to the wireless industry, which turned to the matter in late spring 1997 under the auspices of the Canadian Wireless Telecommunications Association (Canadian Wireless Telecommunications Association. Wireless E9-1-1 Working Group, 1997). In contrast to the FCC mandated approach, Wireless E9-1-1 in Canada was initiated through a voluntary effort between industry players and the public safety community.

By 2002, this voluntary effort had led to the successful deployment of Wireless E9-1-1 with FCC Phase 1 equivalency in a number of Canadian cities. A Canadian version of the FCC Phase 2 equivalent has not yet been contemplated in any public forum, and the future of high-resolution Wireless E9-1-1 in Canada remains uncertain.

Already at least one commercial location-based service has appeared in conjunction with the deployment of Phase 1 Wireless E9-1-1 capabilities. Bell Mobility's *MyFinder* service offers directory information based on the cell-site/sector location of a mobile phone customer (Bell Mobility, 2002). According to its privacy statement any disclosure of location information is strictly on an active consent basis with clear limits on the retention of such information:

When we offer you optional MyFinder services that require use or disclosure, or both, of your cell phone's location and your cell phone number, we will, *first obtain your express consent* before using or disclosing this information. ...

For your convenience, we will retain a record of your last 'Find Me' location request so that you may readily re-access this information. Each new 'Find Me' request deletes the previous record that was retained.

(Bell Mobility, 2003)

Customer Anonymity and Prepaid Mobile Phone Services

Despite the limited success of Phase 1 Wireless E9-1-1 in Canada, its development has not been without difference of opinion among certain interested parties. In fact, a close examination of the process reveals an ironic twist to the tale: the closer the industry and public safety agencies came to implementing a working system, the more they found themselves at odds with one another over the issue of populating the Automatic Location Identification (ALI) database with subscriber list information. The debate was divided among the wireless carriers on one side and the public safety agencies on the other, and boiled down to what type of information was to be placed in the ALI database that would provide emergency operators with the E9-1-1 features. According to standards developed in conjunction with the FCC Phase 1 precedent, the ALI database is to be populated with cell site/sector address information that is then sent to the public safety answering point (PSAP) when an emergency call is placed from a mobile telephone. This design is known in the industry as the Emergency Services Routing Digit (ESRD) solution, which refers to a number assigned to each cell-site/sector and subsequently linked to an address field in

the ALI database.⁹ For the wireless industry this was considered the accepted method for providing Wireless E9-1-1 (FCC Phase 1).

The public safety agencies, however, have sought *real-time disclosure* of wireless subscriber list information, which requires populating the ALI database with the home or business addresses of all wireless customers. Representatives of the public safety community have made their demands known in various forums, drawing on the argument that such information might prove valuable in locating a caller during or after an emergency call. For its part, the wireless industry has countered this demand with the claim that such information is meaningless when calls are placed from mobile phones that essentially have no fixed association with a subscriber's home or business address, or even with a particular individual for that matter. Moreover, suggested the wireless industry, such information could ultimately mislead emergency response personnel and send them to a wrong location. Allegations were even made by one industry stakeholder that the public safety agencies had a hidden agenda with the law enforcement community, characterizing their request as "an ad hoc idea with a checkered past" (Microcell Telecommunications Inc., 2001), although on further inquiry this has proven to be unfounded (CRTC Interconnection Steering Committee Network Security Working Group, 1999).

Nevertheless, the PSAPs persisted in their demands and were initially supported by the CRTC through a directive that required Wireless CLECs to populate the ALI database with their subscriber list information in those operating territories where Wireless E9-1-1 is not available (Canadian Radio-television and Telecommunications Commission, 2000). The wireless industry protested this directive vigorously and the cooperative spirit that had marked the initial development of Wireless E9-1-1 in Canada soon disintegrated into caustic debate and an eventual stalemate between the wireless industry and the public safety agencies.

At this point, in late 2001, the regulator stepped in to examine the issue and to solicit input on the matter of populating the ALI database with the subscriber list information held by the Wireless Service Providers (Canadian Radio-television and Telecommunications Commission, 2001). Several months prior to this intervention a mobile phone operator Microcell Connexions Inc. (under the brand name "Fido") filed plans with the CRTC stating its intention to become a Wireless CLEC (Canadian Radio-television and Telecommunications Commission, 2000). Despite the best intentions of the CRTC to ensure technological neutrality in its regulatory framework, this first attempt to establish a *mobile* Wireless CLEC in Canada has revealed problems with the E9-1-1 obligation as formulated in paragraph 286 of the Local Competition Framework.

Paragraph 286 creates a potential problem of regulatory asymmetry with telecommunications services in Canada because mobile wireless services are problematic when interpreting aspects of the current framework. The public safety agencies used the ambiguity of paragraph 286 to

⁹ Each cell-site or cell-sector (many cellular base stations are divided into three or more zones) is assigned a 10-digit ESRD that resembles a telephone number. The ESRD is delivered to the ALI database where it is cross-referenced with address of the cellular base station. In turn, the physical location of that base station is assigned an Emergency Services Zone (ESZ) that enables a 911 operator to redirect the call to the proper municipal authorities for dispatch.

support a case for including subscriber list information in the ALI database – a case that was initially accepted by the regulator in Order 200-831 describe above.

During the subsequent debate over this obligation, Microcell Connexions, the company applying for Wireless CLEC status, pointed to the problem that prepaid mobile phone service raises with respect to populating the ALI database with verifiable subscriber list information. It noted that its business was predicated on some fifty per cent or more of its customers opting for a prepaid account. Microcell stated in its remarks that prepaid services are frequently offered through third party retailers who are not required to verify customer information and in some cases where prepaid phone packages are sold at convenience stores, retailers may not even collect customer information. In such cases, he Microcell argued that fulfilling the ALI obligation would be onerous undertaking of little practical value and, moreover, that it might in fact violate provisions of Canada's privacy legislation:

[...] we submit that is entirely reasonable and legitimate for a customer to want to limit the disclosure of personal information when subscribing to a service, especially prepaid service where no monthly bill is issued and there is no apparent need for a subscriber address. [...] Microcell submits that is by no means intuitively obvious to a reasonable member of the general public that a fixed address *must* be provided in order to receive mobile phone service. Resistance to providing fixed address information, therefore, is understandable, especially in light of the heightened awareness of privacy rights and concerns over the ability of organizations to protect personal data in the information age.

(Microcell Telecommunications Inc., 2001: 11)

From the perspective of the wireless carriers, E9-1-1 is to provide a functionally equivalent system to the wireline services and thus limited to location and telephone number information only. Personal information in the form of home or business address is considered irrelevant to a mobile service, and possibly unlawful if gathered with respect to prepaid offerings.

In response to Microcell's position, some of the PSAPs put forward the view that customers *do not have a right to anonymity* with regard to any form of mobile phone service:

Microcell would have us [PSAPs] believe they are now experts in privacy law, and their customer's [*sic*] have the right to be anonymous. How many wireline customers have this right, the answer is none.

(Alberta E9-1-1 Advisory Association, 2002)

Prior to making this statement, the PSAPs had previously put forward a recommendation that all new mobile phone customer activations be accompanied by two pieces of photo identification as a way of collecting and verifying the subscriber list information for entry into the E9-1-1 system. Microcell, in opposition, characterized this as an action that would “establish Canada as a wireless backwater compared to other countries’ approach to consumer friendly communications,” suggesting further that such a requirement “is unjustifiable and offensive to

personal privacy” when it comes to prepaid services (Microcell Telecommunications Inc., 2002).

In summer 2003 the CRTC overturned its decision to require wireless CLECs to populate the ALI database with subscriber list information, opting instead for a more sensible approach based on a combination of Phase 1 Wireless E9-1-1 (where available) and a mandate for all wireless carriers to provide the PSAPs with 24/7 telephone access to their security departments (Canadian Radio-television and Telecommunications Commission, 2003). While the obligation to collect and verify subscriber list information for Wireless E9-1-1 service may have been put to rest for the time being, a debate about customer anonymity when purchasing prepaid mobile service may be nonetheless worthy of further consideration as we will discuss in the next section.

Discussion: The Right to Anonymity and Network Enabled Devices

The reluctance of wireless service providers to provide subscriber list information to the public safety agencies suggests that customer privacy concerns cannot be characterized simply in this case, but rather that the issue involves a set of considerations that embody business strategy (i.e., protecting customer data from competitors), the functional value of such information versus the associated costs of collecting it, as well as existing government legislation and restrictions on personal information (e.g., PIPED Act).

Microcell’s concerted effort to demonstrate the problems associated with the collection of prepaid customer information is tempered by events in Australia, where the regulator has placed controls on the purchase of prepaid mobile phone service and now requires service providers to collect verifiable personal identification of customers prior to activation (Australian Communications Authority, 2000). The Australian regulator claims that the anonymity possible with prepaid service was deemed inconsistent under the “obligations of the Telecommunications Act,” and raised concerns with law enforcement and national security agencies.¹⁰

At present in Canada it is not the case that subscriber list information is required for Wireless E9-1-1 service but future regulatory decisions will no doubt continue to set precedent in defining more precisely what the phrase “appropriate end-user information” in paragraph 286 of the Local Competition Framework will come to mean for the future of this service in Canada. The Australian case suggests that despite Canadian opposition to collect customer information for prepaid accounts through an identification requirement, such an approach is entirely feasible and would not necessarily establish Canada as a ‘wireless backwater’ of customer service. In fact, it might just represent an impending debate on which the Privacy Commissioner may be called to issue a judgment, for it is not clear by any means that a requirement for the collection of such information has any purpose *ex ante* for which “a reasonable person,” according to Section 5.3 of the PIPED Act, “would consider appropriate”.

¹⁰ Background to this determination is not readily available on the Australian regulator’s website. Further research needs to be done to look into the circumstance and possible debate that accompanied this requirement in Australia and similar requirements that may exist in other countries.

More generally, the issue of anonymity rights for prepaid mobile phone service is not unlike that raised with regard to certain kinds of Internet services, where personal information can remain distinct from network activity. The owner of personal computer is not typically required to provide verifiable personal information when purchasing the device. When purchasing Internet services a customer may be required to provide personal data for billing purposes but there is no inherent reason that their network identity need be linked to that personal information. Moreover, a person using an Internet café terminal may not be required to provide any form of personal information when conducting online activity. The question we would pose is thus: on principal should prepaid mobile telephone ownership be any different? We might press further too: should requirements for access to telephone service in general be any different from using other networked technologies, such as personal computers or personal digital assistants? Certainly for public safety reasons, a mobile phone subscriber *might* wish to have their name and residential address made available to an emergency operator but this is clearly not a requirement under current definitions of Wireless E9-1-1 service. Likewise, with the advent of Voice over Internet Protocol (VoIP) telephony, there is a similar challenge for the provision of E9-1-1 service to traditional wireline customers, who may wish to preserve their 'online' anonymity.

Lawrence Lessig (1999) describes the civil rights challenge created by the internet as a product of *latent ambiguities* in existing regulatory frameworks. A right to anonymity in ownership of a telephone or telephone number on a public network seems to embody this form of ambiguity. With an increasingly competitive marketplace for telecom services and the continuing growth of the prepaid mobile phone market and emerging next generation offerings that will continue to evolve into more sophisticated portable networked personal computers, regulatory precedents set in this domain may have far reaching consequences for the regulation of other types network enabled devices and thus should be carefully scrutinized by privacy advocates.

References

- Alberta E9-1-1 Advisory Association (2002) Further reply comments submitted pursuant to Public Notice CRTC 2001-110. Canadian Radio-television and Telecommunications Commission.
- Australian Communications Authority (2000) Telecommunications (Service Provider – Identity Check for Pre-paid Public Mobile Telecommunications Services) Determination 2000.
- Bell Canada (2000) ESCOX156: Amendments to the 9-1-1 Trunk-side Interconnection Document to include Wireless CLECs Arrangements, 20 November. CRTC Industry Steering Committee (CISC), Emergency Services Working Group (ESWG).
- Bell Mobility (2002) Bell Mobility introduces MyFinder - Canada's first wireless location based service. 17 December. Retrieved Feb. 1, 2003, from:
<http://www.bce.ca/en/news/releases/bm/2002/12/17/69631.html>

- Bell Mobility (2003) MyFinder. Retrieved Dec. 12, 2003, from:
<http://www.bell.ca/shop/application/commercewf>
- Bennett, C. and P. Regan (2002) What Happens When You Make a 911 Call? Privacy and the Regulation of Cellular Technology in the United States and Canada. Retrieved April, 2003, from: <http://webuvic.ca/polisci/bennett/research/CPSA2002.htm>
- Canadian Radio-television and Telecommunications Commission (1996) Telecom Decision 96-14: Regulation of Mobile Wireless Telecommunications Services.
- Canadian Radio-television and Telecommunications Commission (1997) Telecom Decision 97-8: Local Competition.
- Canadian Radio-television and Telecommunications Commission (1999) Telecom Decision 99-17: 9-1-1 Service – Rates for Wireless Service Providers, Centrex Customers and Multi-Line Customers/Manual Access to the Automatic Location Identification Database., 29 October.
- Canadian Radio-television and Telecommunications Commission (2000) Order CRTC 2000-831: General Tariff approved on an interim basis with modifications for Microcell Connexions Inc., 8 September.
- Canadian Radio-television and Telecommunications Commission (2001) Public Notice CRTC 2001-110: Conditions of service for wireless competitive local exchange carriers and for 9-1-1 services offered by wireless service providers, 31 October.
- Canadian Radio-television and Telecommunications Commission (2003) Decision CRTC 2003-53: Conditions of service for wireless competitive local exchange carriers and for emergency services offered by wireless service providers, 12 August.
- Canadian Wireless Telecommunications Association (2003) Mobile Wireless Subscribers in Canada. CWTA Facts.
- Canadian Wireless Telecommunications Association Wireless E9-1-1 Working Group. (1997). Round-Table Discussion: Wireless 9-1-1 Service Summary of Discussion, 17 June
- CRTC Interconnection Steering Committee Network Security Working Group (1999) NSTF0006: PSAP emergency ALI database lookup for non 9-1-1 dialled emergency calls or for 9-1-1 calls where there is no ALI record and SPID is required. CISC Network Security WG Monthly Status Report, 12 November.
- Electronic Privacy Information Centre (2003) CPNI (Customer Proprietary Network Information). Retrieved December, 2003, from: <http://www.epic.org/privacy/cpni/>

- Federal Communications Commission (2001) FCC Wireless 911 Requirements, January. Retrieved Apr., 2002, from: http://www.fcc.gov/911/enhanced/factsheet_requirements_012001.pdf
- Federal Communications Commission. (2002) FCC takes steps to improve the ability of public safety agencies to assist wireless callers using non-service-initialized phones. FCC News, 29 April. Retrieved Dec. 3, 2003, from: http://www.fcc.gov/Bureaus/Wireline_Competition/News_Releases/2002/nrwc0202.htm
1
- Federal Communications Commission (2003.). Wireless E911 Coordination Initiative, 13 November. Retrieved Nov. 25, 2003, from: <http://wireless.fcc.gov/outreach/e911/>
- Futch, A. and C. Soares (2001) Enhanced 911 Technology and Privacy Concerns: How has the balance changed since September 11? *Duke Law & Technology Review*, 26 October. Retrieved April, 2003, from: <http://www.law.duke.edu/journals/dltr/articles/2001dltr0038.html>
- Gow, G. A. (2002). *Canadian Telecommunications Policy and the National Disaster Mitigation Strategy: Observing Wireless E9-1-1*. Simon Fraser University, Vancouver.
- Hanson, W. (2003) FCC Expands E911 Rules, *Government Technology News*, 17 November. Retrieved Dec. 12, 2003, from: <http://www.govtech.net/news/news.php?id=77512>
- Legal Information Institute (1999) United States Code Title 47: Telegraphs, Telephones, and Radiotelegraphs (Chapter 5, Subchapter II, Part I, Sec. 222: Privacy of Customer Information). *United States Federal Statutes*. Retrieved Dec. 11, 2003, from: <http://www4.law.cornell.edu>
- Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books.
- Microcell Telecommunications Inc. (2001) ESCOX159: Entry of Wireless End-User Subscriber Data into 9-1-1 Automatic Location Information (ALI) Databases. CRTC Industry Steering Committee (CISC), Emergency Services Working Group (ESWG), 1 February.
- Microcell Telecommunications Inc. (2002) Reply comments submitted pursuant to Public Notice CRTC 2001-110. Canadian Radio-television and Telecommunications Commission.
- National Emergency Number Association (2002a) 9-1-1 Facts. Retrieved Mar. 30, 2002, from: http://www.nena9-1-1.org/PR_Publications/Devel_of_911.htm

National Emergency Number Association (2002b) 9-1-1 Tutorial, 31 January. Retrieved Apr. 8, 2002, from: http://www.nena.org/9-1-1%20Tutorial/9-1-1_tutorial.htm

Phillips, D. (2003) Beyond Privacy: Confronting Locational Surveillance in Wireless Communication, *Communication Law and Policy*, 8(1), 1-23.

Privacy Commissioner of Canada (2000) Personal Information Protection and Electronic Documents Act. Retrieved Dec. 12, 2003, from: http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp

Privacy Commissioner of Canada (2003) *Commissioner's Findings*. Retrieved Dec. 11, 2003, from: <http://www.privcom.gc.ca>

Regan, P., C. Bennett and D. Phillips (2002) Emergent Locations: Implementing Wireless E9-1-1 in Texas, Virginia, and Ontario. Paper presented at the Telecommunications Policy Research Conference, 28-30 September, Alexandria, VA.

Sparks, S. (2000) Opting in is out: Balancing Telecommunications Carrier Commercial Speech Rights With Consumer Data Privacy, *International Journal of Communications Law and Policy*. 14 July. Retrieved Nov. 14, 2003, from: http://www.ijclp.org/5_2000/ijclp_webdoc_7_5_2000.html

Wireless Location Industry Association. (2001) WLIA Online. Retrieved April, 2002, from: <http://www.wliaonline.com>