Pinpointing Consent: Location Privacy, Public Safety, and Mobile Phones

Gordon A. Gow

Pinpointing Consent: Location Privacy, Public Safety, and Mobile Phones

Gordon A. Gow[1]
Department of Media and Communications
London School of Economics and Political Science
London WC2A 2AE

tel: +44 (0)207 955 7695
fax: +44 (0)207 955 7248
g.gow@lse.ac.uk

Paper prepared for 'The Global and the Local in Mobile Communication' conference. Institute for Philosophical Research of the Hungarian Academy of Sciences; Budapest, June 10-11, 2004.

ABSTRACT

Accompanying the growing interest in emerging location based services has been an urgent but rather ambiguous concern shared among scholars, privacy advocates and the general public that enhanced safety will come at the expense of personal privacy. Precision tracking of mobile devices has raised the spectre of unwanted and pervasive surveillance from both state and commercial interests. This juxtaposition of public safety with fears over loss of privacy raises important questions about appropriate collection, use, and disclosure of personal information in the context of mobile phone services and network-enabled devices in general. This paper will report on findings from an ongoing study that is looking at initiatives to introduce location-based services for public safety in the United States, Canada, and Europe. It will address a number of aspects of these developments by drawing on official regulatory and policy sources. In particular, this paper will examine the various legal and regulatory aspects related to the conditions by which "consent" is established for collection, use, and disclosure of location information generated by mobile phones and other mobile access technologies.

---

[1] Gordon Gow is a Lecturer in the Department of Media and Communications at the London School of Economics and Political Science, as well as Director of the MSc Programme in Media and Communications Regulation and Policy. Among other things, his research examines the social impact of mobile communications from a regulatory and policy perspective, emphasizing public participatory approaches to technology assessment and risk management. He has published on the issue of Wireless E9-1-1 and prepaid mobile phone service in the journal *Surveillance & Society*. This paper represents an extension of that earlier work along a new axis of inquiry.

Introduction

Some of the earliest progress in the area of location-based services is a direct result of the American public safety initiative known as wireless 'enhanced' 9-1-1. Wireless E9-1-1 has been driven forward by an FCC mandate to deliver widespread capability for location-based services in the United States by 2005. In other parts of the world location-based services are also unfolding in conjunction with public safety initiatives—'CGALIES' in the EU and 'MoLI' in Australia—prompting reports in the media where we find the promise of enhanced personal safety tempered by fears over loss of privacy and unwanted pervasive surveillance.

Contrary to the assumptions we often find in media reports, a central premise of this paper is that location information unto itself is not personal information *per se* but that it becomes such only when coordinated with other kinds of information. A major debate in the issue over location privacy is thus about consent—the terms and conditions by which location information may be collected and combined with other details to produce personal profiles for public safety or commercial purposes. This networking of personal information may be the necessary step in providing commercial services that add real value to otherwise raw location data:

> … knowledge of the user's location is only part of the problem. Depending on where, when, how, with whom, and why customers are navigating in physical space, their needs will vary. … Even if the LBS [location-based services] provider was able to push information or advertising with great reliability to these customers, they might have an extremely difficult time figuring out what the customer is doing or want at that location in real time.
> … There is an urgent need for sophisticated mobile marketing techniques based on detailed knowledge of customer profiles, history, needs, and preferences. Information existing in customer databases developed by retailers like Amazon.com, for example, can be used in parallel with location-based information. (Rao & Minakakis, 2003)

Optimist forecasts have placed the market for LBS at over $32 billion in Europe alone by 2005, with a global reach of 680 million customers (Rao & Minakakis, 2003). As the excerpt above is intended to show, however, much of the value proposition for these services will rely less on the provision of location data and more on the ability of service providers to establish connections across multiple customer databases located in different domains. The terms and conditions by which these connections may be rightfully made raises the matter of customer consent, which it turns out may not be as straightforward as one might expect. In this paper I will first present an analytical framework based on a number of key distinctions in the field of location privacy and then draw upon it to examine the issue of consent in three distinct settings: the United States, Canada and the European Union. The terms and conditions by which consent is deemed granted in these regions will likely have significant implications for personal privacy and the future development of mobile data services within and across borders.

Location Privacy

David Lyon (Lyon, 2003) has argued that bureaucratic surveillance is a hallmark of the modern era but that two major changes appear to have inaugurated a new historical moment: the first being the advancement of surveillance techniques through large scale computerization; the second being the entry of commercial organizations into the fray those social institutions motivated and committed to undertake systematic surveillance of the population. Lyon (p. 164) sees these two developments as characteristic of an emerging postmodern surveillance society. In many respects, the mobile phone may be

the perfect symbol for this new society, especially to the extent that the convergence of a small mobile computer with commercial service providers has created an environment ripe for pervasive personal surveillance.

Among the panoply of concerns about pervasive surveillance is an emerging area now being referred to as one of 'location privacy' (White, 2003). Location privacy is a social, regulatory and policy issue that has emerged with the appearance of location-aware mobile phones and the advent of location-based services for public safety and commercial purposes.[2] Recent media coverage of location-based services for public safety illustrates a widespread ambiguity with respect to the issue of location privacy. On the one hand, consumers and privacy advocates are fearful of the potential of unwanted pervasive surveillance. On the other hand, both also recognize the public safety benefit as well as commercial and cultural possibilities of location tracking technology. But is it that by simply owning a location-enabled mobile phone that one's privacy is in jeopardy? In some cases the media appears to draw on this naïve assumption to heighten the drama of this new technology:

> Mobile phone users can be tracked from web site—no more "I'm working late" for UK mobile users. …
>
> … That dinky little Nokia in your pocket could be your undoing if you're up to no good. (Rouse, 2003)
>
> Big Brother's here, on your cellphone (Chatterjee, 2003)
>
> Cellphones: No place to hide (Charny, 2002)

[2] It is important to note that mobile phone service has pretty much always been 'location-aware' to the extent that the service provider's network must be able to track their customers devices as they roam from cell-site to cell-site, or city to city. This most basic tracking capability provides the necessary functionality for enabling handoffs, regional roaming, and customer billing. The new era of location-aware devices offer much higher resolution in tracking the geographic whereabouts of customer devices and has promotes commercial business models of value-added applications based on that capability.

In order to understand how location information enters into the realm of personal privacy concerns a number of factors need to be considered. For example, White (White, 2003) distinguishes location privacy issues from other related information privacy concerns by three discrete operations. The first of these is the gathering of location information, the second is the use of data processing applied to that information to make it useful, and the third is the application of that information to enhance commercial or public safety services.

White's model is a useful starting point for establishing a framework to consider location privacy concerns but it can be further enhanced if combined with existing regulatory approaches for assessing information privacy more generally. For example, much legislation on information privacy recognizes three distinct activities: (1) the initial *collection* of personal information and (2) subsequent *use* and (3) *disclosure* of that information. It is not necessarily the case that the gathering of location information is equivalent to the collection of personal information, although it has been argued elsewhere that they should be regarded as equivalent (Green & Smith, 2004). Nevertheless it is clearly the case that the gathering of location information and its use and disclosure in combination with other customer details—what Wallace (Wallace, 1999) has termed the 'coordinability' of identity traits—could provide the basis for the creation of personal, even intimate, profiling of customers and users of a communications service. The potential availability of such profiles is of considerable interest to law enforcement, national security and commercial organizations. Personal privacy is thus relegated into two distinct policy areas, one stemming from state interests and referred to as 'lawful access' provisions, the second to private commercial interests in the area of

'electronic commerce.' In this paper both areas will be touched upon, although emphasis will be on documents dealing with electronic commerce.

Within each operation we can identify a number of additional factors that will determine the degree to which location information may be coordinated with other personal data. In the case of the gathering of location information one key factor in determining coordinability is the degree of anonymity in the customer-carrier relationship. Typically a carrier will require a customer to provide their name, address, banking and credit information, etc. in order to establish a commercial relationship. With a prepaid mobile phone it is possible to establish full or nearly full anonymity in the customer-carrier relationship. However, in some situations it may be possible to reveal customer identity through even a prepaid service depending on how the phone is used. Imagine an m-commerce transaction using a customer's credit card number. It may be possible in this circumstance to collect location information related to the transaction and then reveal personal details about the customer by linking the credit card number to the mobile telephone number.

Nevertheless, a customer could in principle control the collection of this kind of location information during m-commerce transactions or the collection of high-resolution location information (e.g., GPS-capable handsets). For example, m-commerce transactions using anonymized electronic cash might be conducted through a mobile phone without the need to reveal the vendor, spender, or the location of the transaction. Customers might also choose to switch off the location-aware functionality in their phones if they wish to prevent passive transmission of their precise location to their service provider.

With data processing operation, a related consideration is the extent to which the carrier is capable of establishing relationships within the various types of 'identity knowledge' (Marx, 1999) provided in the customer-carrier relationship including traffic information and collected location data.[3] The greater the range of identity knowledge that can be coordinated with traffic information, the greater the capability to generate detailed personal profiles linked to location information. The most basic coordination is between customer traffic data and customer name and address for simple billing purposes. Where a customer has provided additional personal information to their carrier—perhaps at the point of sale or with the encouragement of a rewards scheme—the possibilities for coordination of identity traits grows in direct proportion (e.g., banking details, names of friends and associates who have acted as referrals, employer, education level, etc). Coordination of identity traits depends on a number of related factors: locations of stored data (single or multiple databases, linked/unlinked), access policies for captured data (who, what, when, how, why), and retention policies for captured data.

Disclosure of information to third parties for value-added applications hinges on the central factor of customer consent. Consent may also apply within the customer-carrier relationship to the extent that it is required to use personal information details to provide customers with internal marketing and special services. Consent is typically described as an opt-in or opt-out regime, where the opt-in regime requires that a customer specifically allows (sometimes on a per use basis) disclosure of their location information for third party applications. Concerns about location privacy with Wireless E9-1-1 in North America typically focus on the issue of consent as it pertains to the disclosure of

[3] Marx lists seven types of identity knowledge.

information about the location of mobile phones operating on a wireless carrier's network (Futch & Soares, 2001; Phillips, 2003; Regan, Bennett, & Phillips, 2002).

Consent in the United States

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 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 dialled, 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).

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 coordinability of personal information with location data. According to its definition in current American legislation is 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.

In 2003 the Wireless Privacy Protection Act was proposed in response to concerns over the control of location data within the existing CPNI regime. This bill, which appears to have now been referred to Congressional Committee on Energy and Commerce of the United States, aims to require customer consent in all instances of non-emergency use of wireless call location. A similar bill, the Location Privacy Act of 2001, died on the house floor in the wake of the events of September 11 and the FCC later rejected a similar proposal by the Cellular Telecommunications Industry Association on the grounds that it was unnecessary (Mobile Communications Report, 2002; Vaughn, 2002).

Consent in Canada

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 Canadian regulator has established 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" (Canada. 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 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, 2000). The application of the Act currently applies to all federally regulated commercial organizations, including telecommunications service providers. 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.

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.

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 it customers, and indeed in a number 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.

In 2002 the Privacy Commissioner's office issued a position on the requirement to collect subscriber list information as a condition of service. In a letter to the three federal departments that sponsored a set of 'Lawful Access' proposals intended to reform various pieces of legislation affecting Canadian's rights to privacy, Privacy Commissioner George Radwanski effectively rejected most of the proposals stating that '(t)he arguments advanced in the consultation paper are completely insufficient' and called into question the impetus behind it:

> What's missing [from the proposals] is evidence demonstrating that there is, in fact, a serious problem that needs to be addressed. Lacking any evidence of serious problems requiring correction by invading the privacy of Canadians, it is not possible to be persuaded that the proposals address these problems effectively, proportionally, and in the least privacy-invasive manner possible. (Office of the Privacy Commissioner of Canada, 2002)

One the last point, Radwanski is referring to a four-part test he has suggested when new intrusions or limitations on privacy are proposed. Essentially the test asks if the measure is: demonstrably necessary; if it is demonstrably effective in achieving its intended purpose; if its intrusion on privacy is proportional to the gained security benefit; and if it is demonstrated that no other suitable and less invasive measures 'would suffice to achieve the same purpose.'

More specifically, with regard to wireless telecommunications, the Privacy Commissioner takes exception to the claim in the proposals that telecom traffic data involves a lower expectation of privacy especially because it includes 'a record of the location of the cell phone in question as it moves about from cell to cell.' On this basis he concludes that such traffic data 'is far more personal and revealing' than presumably wireline generated traffic. He subsequently rejects arguments for creating new measures for data retention and production orders.

This seems a reasonable position based on conserving the status quo in the face of pressure to make changes in light of technological developments; however, it masks the fact that most wireline customers do consent as part of standard practice to the collection of subscriber list information as a condition of service. On the face of it this seems to contradict his position on the predisposition of customer consent, except in the case of prepaid telecom services where there is no apparent reason to collect customer information if payment is made in cash.

Consent in the EU

The situation in European Union is similar to that in Canada and United States insofar as the right to privacy is temporarily waived and consent is implied during emergency situations. For regulatory purposes, an emergency situation is assumed to exist when a customer dials 9-1-1 in North America or 1-1-2 in most European centres. Article 10 of the EC Directive on Privacy and Electronic Communications (2002/58) requires a transparent process governing the use and disclosure of location information while directing service providers to ignore

> … the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls. (European Parliament and the Council of the European Union, 2002)

Initial efforts toward a European Wireless E1-1-2 system began in 2000, with the formation of the Coordination Group on Access to Location Information for Emergency Services (CGALIES). Official policy at the EU level has been to leave it to industry voluntary efforts in the hope that commercial interests in location-based services would provide a strong enough incentive to establish the technical capability needed to support Wireless E1-1-2 within a reasonable timeframe.

The EU, like the regulatory body in Canada, has so far avoided a sweeping American FCC-styled mandate, preferring to leave development of technical capability for location-based services in the hands of commercial interests. Despite this laissez-faire policy in technical matters, however, the Commission has made it obligatory for operators to forward caller location to the extent that it is technically feasible. The

obligation is found in article 26 from Directive 2002/22/EC, yet it does not appear to make a designation between various types of operators that are now established in the telecom sector. One must assume, then, that subject to this obligation are all incumbent wireline carriers, new entrants in both wireline and wireless, and presumably emerging services such as Mobile Virtual Network Operators (MVNOs) and voice over Internet Protocol (VoIP) operators.

This obligation is similar to the Canadian approach—but with a significant difference insofar as it only applies to operators in Canada are that are subject to regulatory oversight. Most wireless service providers in Canada operate under regulatory forbearance and so are not obliged to provide Wireless E9-1-1 services (although most now have chosen to do so voluntarily). In Canada it is therefore unclear if the same terms and conditions (described above) for customer consent regarding the disclosure of customer information to emergency services by regulated operators apply to those operators under the forebearance regime. On the face of it they would not, which suggests a situation of regulatory asymmetry in Canada with regard to customer consent in the disclosure of personal information to emergency services. The EU seems to have avoided this problem by issuing a blanket directive but it is not clear if discrepancies will appear when the obligation is transposed into regulatory frameworks of member states.

With regard to commercial use and disclosure of location information, commentators on the EU Directive have been of mixed opinion concerning its protection of personal privacy. A briefing paper from the Internet Society, for instance, suggests that compared with the United States, 'the regulatory situation in European Union countries is much clearer' and points toward Article 9 which 'unambiguously requires

informed opt-in consent for the provision of telecommunications services based on use of location information' (Ackerman, Kempf, & Miki, 2003). Critical assessments of the Directive have argued that its attempt to remain technology neutral has only led to ambiguity and confusion concerning the collection, use, and disclosure of personal information (Escudero-Pascual & Hosein, 2004). Indicative of this ambiguity is the problem of establishing a clear distinction between 'traffic data' and 'location data.' The document sets out separate definitions for these in Article 2 but seems to confuse the matter in item 35 of the Directive's preamble, where it reveals quite plainly that such a distinction is not clear cut in the case of mobile telecommunications:[4]

> In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. … (European Parliament and the Council of the European Union, 2002)

The ambiguity not only reveals the difficulties and possible inadequacy of attempting to maintain technology neutral language but it may have far reaching implications for customer consent and pervasive use of location data. For example, if location data is deemed to be traffic data then it may be subject to an erasure requirement (articles 6.1 and 6.3) and operators will need to inform customers of the use of location data as well as 'the duration of such processing' (article 6.4). If, however, such data is deemed to be 'location data' under article 9 then operators are required to either make the data anonymous or to obtain 'the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value-added service.' In obtaining consent,

---

[4] Items 14 and 15 in the pre-amble attempt to clarify the difference between location data and traffic data, further illustrating the difficulty of making this distinction.

operators must inform customers as to the terms and conditions of use and disclosure of the location data. Yet article 9 does not mention an erasure requirement, which appears to suggest that 'location data' (as opposed to 'traffic data') may be held for indefinite period of time. The failure to establish a clear distinction between these terms in the Directive creates a potential loophole through which commercial interests may tailor their collection and use of customer data.

A recent paper on E112 in Europe (Rodriguez Casal, 2003) has raised a different matter regarding consent, observing that it may in fact be 'easily obtained' by companies offering incentive schemes or by asking for blanket consent on a bundled package of services that may not be offered separately. The Directive does not appear to address this possibility. Furthermore, the Directive may actually contain an ambiguity with its opt-in requirement not unlike that discussed above in the US case. (You will recall that the opt-in under the Wireless Communications and Public Safety Act now effectively means 'opt-out' according to FCC interpretation of CPNI rules more generally).

To understand this, we need to first recognize that Article 9 requires customers to actively opt-in for service but places no specific limitations on the extent to which this consent may apply. Article 9, paragraph one, simply states 'to the extent and for the duration necessary' for the provision of the service. An operator that encourages customers to opt-in to a blanket provision for use of their location data as part of their overall service package may effectively gain that consent on a going forward basis. Is this a possible scenario? Well, according to item 17 of the Directive's pre-amble, consent 'may be given by any appropriate method enabling a freely given specific and information indication of the user's wishes, including by ticking a box when visiting an

Internet website.' A lengthy privacy policy statement with a carefully worded and deeply buried consent clause could certainly go a long way to ensuring that many if not most customers would unknowingly opt-in to a blanket provision for use of their location data.

Now combine that possibility together with article 9 paragraph two, which requires operators who have obtained this prior consent to subsequently allow customers the option of 'refusing the processing of such data for each connection to the network or for each transmission of communications.' This provides customers with opt-out but on a call-by-call basis only (similar to a customer's right to withhold caller-ID information on a call-by-call basis). When combined with the blanket provision possibility from paragraph one, it seems that the Directive may leave open the possibility of a *de facto* opt-out regime not unlike the currently ironic situation in the United States—if customers opt-in to a blanket consent provision they are effectively entering into a per-call, opt-out arrangement with their service provider. Such a possibility is not yet evident in practice and its feasibility will depend on how the Directive has been transposed into national regulatory frameworks.

Conclusion

In this paper I have argued that location information is not personal information *per se* but only become so when combined with other identity traits. As such, consent establishes the legal grounds for the coordinability of identity traits and is therefore paramount in understanding location privacy issues. I have introduced a process model used by information privacy advocates and researchers that distinguishes between three moments of consent in the collection, use, and disclosure of personal data. What is

evident when we draw upon this model to compare regulatory and policy sources from the United States, Canada, and Europe is that much of the current focus is on the use and disclosure moments, rather than collection in the first instance.

Consent of use and disclosure for emergency purposes consent is unproblematic insofar as it is waived when a user chooses to dial for help. This is the same in the US, Canada, and Europe. However, in the case of electronic commerce the issue of consent is far from clear owing in part to the problem of distinguishing traffic data (CPNI) from location data. Part of this problem stems from efforts to word current legislation in technology neutral terms. In the Canadian case, the Privacy Commissioner has addressed the issue of consent in the initial collection of customer data, moving the debate beyond the use and disclosure moments and challenging the legitimacy of service providers demanding certain forms of personal data as a condition of service. Recent news about the Swiss government's move to eliminate anonymous prepaid mobile phone service (Swissinfo, 2004) illustrates the problematic nature of requiring consent during the moment of initial data collection. It appears, given current arrangements, that 'consent' is not a simple matter, but in fact is an entry point into some of the most fundamental challenges that mobile communications services, and more generally digital convergence, present to current policy frameworks and initiatives.

References

Ackerman, L., Kempf, J., & Miki, T. (2003). *Wireless Location Privacy: Law and Policy in the U.S., EU and Japan* (No. 15, ISOC Member Briefing): Internet Society.

Bell Canada. (2000, Nov. 20). ESCOX156: Amendments to the 9-1-1 Trunk-side Interconnection Document to include Wireless CLECs Arrangements. *CRTC Industry Steering Committee (CISC), Emergency Services Working Group*

(ESWG). Retrieved Feb. 12, 2002, from http://www.crtc.gc.ca/cisc/COMMITTE/E-docs/ESCOX156.doc

Bennett, C., & Regan, P. (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.

Canada. Canadian Radio-television and Telecommunications Commission. (1999, Oct. 29). 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. Retrieved Apr. 3, 2002, from http://www.crtc.gc.ca/archive/eng/Decisions/1999/DT99-17.html

Charny, B. (2002, July 26). Cell phones: No place to hide. *ZD Net News*. Retrieved July 26, 2002, from http://zdnet.com.com/2100-1105-946264.htmml

Chatterjee, A. (2003, May 20). Big Brother's here, on your cellphone. *Economic Times (India)*. Retrieved May 20, 2003, from http://www.economictimes.indiatimes.com

Escudero-Pascual, A., & Hosein, I. (2004). Questioning Lawful Access to Traffic Data. *Communications of the ACM*, 47(3), 77-82.

European Parliament and the Council of the European Union. (2002). Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Communities*.

Futch, A., & Soares, C. (2001, Oct. 26). Enhanced 911 Technology and Privacy Concerns: How has the balance changed since September11? *Duke Law & Technology Review*. Retrieved April, 2003, from http://www.law.duke.edu/journals/dltr/articles/2001dltr0038.html

Green, N., & Smith, S. (2004). 'A Spy in your Pocket?' The Regulation of Mobile Data in the UK. *Surveillance & Society*, 1(4), 573-587.

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

Lyon, D. (2003). Surveillance Technology and Surveillance Society. In T. Misa, P. Brey & A. Feenberg (Eds.), *Modernity and Technology* (pp. 164-183). Cambridge, Mass: The MIT Press.

Marx, G. T. (1999). What's in a Name? Some Reflections on the Sociology of Anonymity. *The Information Society*, 15, 99-112.

Mobile Communications Report. (2002, August 5). FCC turns down CTIA petition on wireless location privacy rules. *Wireless Week*. Retrieved Aug. 5, 2002, from http://wirelessweek.com

Office of the Privacy Commissioner of Canada. (2002, Nov. 25). Privacy Commissioner's reply comments regarding the "Lawful Access" proposals. Retrieved Apr. 19, 2004, from http://www.privcom.gc.ca/media/le_021125_e.asp

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

Rao, B., & Minakakis, L. (2003). Evolution of Mobile Location-based Services. *Communications of the ACM*, 46(12), 61-65.

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

Rodriguez Casal, C. (2003). Location and personal information for direct marketing: Third generation killer application. *info*, 5(2), 45-50.

Rouse, A. (2003, March 25). Mobile phone users can tracked from web site--No more "I'm working late" for UK mobile users. *The Inquirer (UK)*. Retrieved Mar. 25, 2003, from http://www.theinquirer.net

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

Swissinfo. (2004, March 4). Swiss phone cards help trace al-Qaeda. *swissinfo.org*. Retrieved Apr. 14, 2004, from http://www.swissinfo.org/sen/Swissinfo.html?siteSect=111&sid=4763869

Vaughn, A. (2002, August 1). Privacy Ruling Falls Flat with Industry. *Wireless Week*. Retrieved Aug. 1, 2002, from http://www.wirelessweek.com

Wallace, K. (1999). Anonymity. *Ethics and Information Technology*, 1, 23-35.

White, J. C. (2003). *People, Not Places: A Policy Framework for Analyzing Location Privacy Issues* (Masters Memo Prepared for the Electronic Privacy Information Center): Terry Sanford Institute of Public Policy, Duke University.