Canadian Journal of Law and Technology

Volume 7
Number 1 *1 & 2*

Article 7

1-1-2010

Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy

Teresa Scassa

Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy

Teresa Scassa*

INTRODUCTION

Location information can be broadly defined as any data which places one at a particular location at any given point in time, or at a series of locations over time.[1] Location data can be used singly or in combination to create a data picture of one's movements in public space.[2] There are myriad ways in which individuals leave location data in the hands of private sector organizations.[3] ATM records and receipts of electronic transactions in shops both provide information about one's activities at particular points in time and space, as do cell phones,[4] surveillance camera footage, and RFID data.[5]

---

* Canada Research Chair in Information Law, University of Ottawa, Faculty of Law, Common Law Section. I gratefully acknowledge the support of the GEOIDE Network and the Canada Research Chairs program. I gratefully acknowledge the research assistance of Kelly Harris. Many thanks to Elizabeth F. Judge for her comments on an earlier draft of this paper.

1 Note that this definition is different from some definitions in works that focus more specifically on privacy issues with location based services. See e.g. David Lyon, Stephen Marmura & Pasha Peroff, *Location Technologies: Mobility, Surveillance and Privacy*, Queen's University: The Surveillance Project (March 2005) at 6, online: The Surveillance Project <http://www.surveillanceproject.org/files/loctech.pdf>. A narrower definition permits a focus on those technologies that permit tracking in real time. A broader definition is chosen here because the discussion is about both the impact of adding location data to other information about an identifiable individual and about the expectation of privacy that individual might have in activities taking place in the spaces identified by that location data.

2 Anne Uteck considers as well the implications of ubiquitous computing for the fine-grained tracking and monitoring of daily activities. See Anne Uteck, "Ubiquitous Computing and Spatial Privacy" in Ian Kerr *et. al.*, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford: Oxford University Press, 2009) at 83–102, online: On the Identity Trail <http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_05.pdf>.

3 For a detailed discussion of technologies relying upon location based information, see Sjaak Nouwt, "Reasonable Expectations of Geo-Privacy?" (2008) 5:2 SCRIPT*ed* 375, online: <http://www.law.ed.ac.uk/ahrc/script-ed/vol5-2/nouwt.pdf>.

4 Mobile Location Systems can work with cell phones to give a precise position for a cell phone. This type of technology has advantages for the delivery of emergency services, but raises privacy concerns as well. See e.g. Nouwt, *supra* note 3.

5 See Teresa Scassa *et al.*, "Consumer Privacy and Radio Frequency Identification Technology" (2005-2006) 37 University of Ottawa Law Review at 215–248. RFIDs that

Increasingly, we are invited to leave even more detailed location data trails. Individuals can enable tracking features on handheld mobile devices so that they can use the device as a navigation system that can offer them route directions as well as local merchant information.[6] Users of such devices will leave a record of their movements and activities for the periods of time in which the application is enabled. Individuals are also increasingly invited to enable tracking applications on hand held devices so as to permit selected "friends" to be able to track their movements and activities.[7] Enabling these features also leaves a trail of location data in the hands of the service provider. Typically, the collection, use and disclosure of this information by the service provider is governed by a user agreement. The terms of the agreement, and any associated privacy policy, may or may not address what the company's position is with respect to requests from law enforcement to access to data about individual users.[8] As will be discussed below, the nature, variety and volume of location data that is collected about individuals, in all of these different contexts, is significant and growing. Kerr *et al.* describe the "universalization of such data collection processes" as "soft surveillance."[9]

The sheer volume of location data that is now being collected by private sector companies in relation to a wide range of products and services poses serious challenges for privacy and data protection law. This article considers a central challenge to privacy posed by the collection and compilation of location data — the accessibility of this data to law enforcement agents through exceptions to the general principles of consent for disclosure that exist under private sector data protection legislation in Canada. Recent court interpretations of these exceptions — primarily in the internet context — paint a muddled picture of their relationship to the right to be free from unreasonable search and seizure under the *Canadian Charter*

---

leave location data trails include those in automated bridge or highway toll passes, and in swipe cards that permit entry into secured areas. RFID-enabled identity documents may also leave data trails. As the use of RFID across a whole range of goods becomes more common, the trail of location data may expand.

6 For example, TomTom, the popular seller of GPS systems, advertises an application that will tell drivers where to find the lowest fuel prices in their area, online: TomTom <http://www.tomtom.com/services/service.php?id=12>.

7 Google Latitude is one of many such applications, online: <http://www.google.com/intl/en_us/latitude/intro.html>. Others include GypSii, online: <http://www.gypsii.com/>, Whrrl, online: <http://whrrl.com>, and Loopt, online: <http://www.loopt.com/>.

8 For a discussion on the formal and informal practices of information sharing with authorities in the Canadian private sector, see Tamil Israel *et al.*, "Personal Information Protection in the Face of Crime and Terror: Information Sharing by Private Enterprises for National Security and Law Enforcement Purposes" (March 2008) Centre for Innovation Law and Policy, online: Centre for Innovation Law and Policy <http://www.innovationlaw.org/Assets/Privacy+report.pdf>.

9 Ian Kerr *et al.*, "Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent" in Ian Kerr, *et al.*, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford: Oxford University Press, 2009) at 5–22, online: <http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_Kerr_01.pdf>.

of Rights and Freedoms.[10] This article considers whether the permissive disclosure provisions of the *Personal Information Protection and Electronic Documents Act*[11] (PIPEDA) and its substantially similar counterparts mean that law enforcement agents have ready access to information about our movements and activities, or whether s. 8 of the *Charter* plays a role in limiting the circumstances in which disclosure without notice or consent may take place.

Section 8 of the *Charter* guarantees only the freedom from *unreasonable* search and seizure. Thus, this section only applies where there is a *reasonable* expectation of privacy.[12] The existence of a reasonable expectation of privacy is, thus, the first issue in considering the application of s. 8 to location data in the hands of third parties. While information about one's movements and activities seems, *prima facie*, to be "core biographical information", there is a risk that the apparently public nature of many of these activities eliminates or reduces any reasonable expectation of privacy. The first part of this article addresses this possibility, and argues that even if one were to accept that there is no reasonable expectation of privacy in public space, there is generally a reasonable expectation of privacy in recorded data about one's movements.

The second part of the article assesses the impact of data protection legislation on the constitutional issues. Cases involving cell phone data, as well as the recent and controversial case law relating to internet service providers' disclosure of subscriber information to police without warrants suggests that, while s. 8 of the *Charter* may play some role in limiting disclosure without consent, complicating factors may include the terms of the company's privacy policy, the wording of the statutory exception, the nature of the information sought, and the court's conception of the information at issue and its significance. This article considers the impact that the proposed Bills C-46 and C-47, the *Investigative Powers for the 21st Century Act* and the *Technical Assistance for Law Enforcement Act* (BILL C-47),[13] would have in this context, and concludes with an assessment of the state of the current law.

---

10 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11, s. 8.

11 S.C. 2000, c. 5 [*PIPEDA*].

12 *Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.*, 1984 CarswellAlta 121, *(*sub nom. *Hunter v. Southam Inc.)* [1984] 2 S.C.R. 145, ¶159 (S.C.C.) [*Hunter*].

13 Bill C-46, *An Act to amend the Criminal Code, the Competition Act, and the Mutual Legal Assistance in Criminal Matters Act*, 40th Sess., 2nd Parl., 2009 [Bill C-46]; Bill C-47, *An Act regulating telecommunications facilities to support investigations*, 40th Sess., 2nd Parl., 2009 [Bill C-47], online: Parliament of Canada <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4007628 &Language=e&Mode=1&>.

I. THE REASONABLE EXPECTATION OF PRIVACY IN PUBLIC SPACE

Courts have frequently found that individuals have little or no expectation of privacy with respect to activities they carry out in public space.[14] Those who have "voluntarily exposed themselves to public gaze"[15] are said to have little basis for complaint if their behavior is observed by others.[16] To frame it another way, "a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place."[17]

Section 8 of the *Charter* guarantees freedom from "unreasonable search and seizure" by agents of the state. In *Hunter v. Southam Inc.*,[18] Chief Justice Dickson of the Supreme Court of Canada stated:

> The guarantee of security from *unreasonable* search and seizure only protects a *reasonable* expectation. This limitation on the right guaranteed by s. 8, whether it is expressed negatively as freedom from "unreasonable" search and seizure, or positively as an entitlement to a "reasonable" expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.[19]

The reasonable expectation of privacy is an objective standard, and it depends not just upon what the affected individual expects in relation to her privacy but also on what the reasonable person would expect in the circumstances. Therefore, it could be argued that, as the use of certain technologies becomes more widespread and more powerful, the reasonable expectation of privacy in public places will necessarily diminish. This includes not only obvious surveillance of public spaces through technologies such as video surveillance, but also the ever-increasing data trails we leave as we surf the internet, bank, shop, dine out, travel, or simply talk on the phone. The very activities that intrude on consumer privacy become illustrations of how consumers have no expectation of privacy.[20]

---

14 See e.g. *Druken v. R.G. Fewer & Associates Inc.* (1998), [1998] N.J. No. 312, 171 Nfld. & P.E.I.R. 312, 1998 CarswellNfld 289, ¶43 (Nfld. T.D.) [*Druken*]. See also *R. v. Shortreed* (1990), 54 C.C.C. (3d) 292 (Ont. C.A.); *R. v. Dilling* (1993), 84 C.C.C. (3d) 325 (B.C. C.A.); leave to appeal refused (1994), 31 C.R. (4th) 406 (note) (S.C.C.); *R. v. Hounsell* (1994), [1994] N.J. No. 319, 1994 CarswellNfld 343 (Nfld. Prov. Ct.); *R. v. Abbey* (2006), [2006] O.J. No. 4689, 2006 CarswellOnt 7381 (Ont. S.C.J.).

15 *Gill v. Hearst Publishing Co.*, 40 Cal. 2d 224, 253 P. 2d 441 (1953). For a detailed and comparative discussion of this issue, see Elizabeth Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 U. T. L .J. 305.

16 *Silber v. British Columbia Television Broadcasting System Ltd.* (1985), [1986] 2 W.W.R. 609 (B.C. S.C.); *Druken*, *supra* note 14.

17 *R. v. Stillman*, [1997] 1 S.C.R. 607, ¶40 (S.C.C.).

18 *Supra* note 12.

19 *Ibid.* at 159-160. Emphasis in original.

20 Nouwt, *supra* note 3 at 395, also notes that the "reasonable expectation of privacy" norm creates the risk of erosion of privacy as technology advances. Stanley A. Cohen,

It is not just the ever-increasing recording of our daily activities that arguably erodes our expectation of privacy; where state purposes such as law enforcement and national security become accepted as necessarily overriding private interests in a growing range of contexts, the reasonableness of any expectation of privacy may be further diminished.[21] It becomes (arguably) no longer reasonable to expect privacy, because technology, combined with an apparent social acceptance of surveillance for security purposes, means that individuals can be taken to have surrendered all or part of their privacy interests in those contexts. Stringham suggests that "[w]hen state surveillance uses ubiquitous technologies, constitutional privacy protection may be diminished as social conventions have already adapted to them."[22]

Yet, the Supreme Court of Canada has cautioned that the reasonable expectation of privacy should not turn on the reasonableness of one's expectations in a context in which privacy is increasingly eroded by technologies of surveillance and data collection. Rather, the analysis should focus on the balance between one's privacy interests and other compelling public interests.[23] As Cohen notes, "[t]he fact that an area is public should not lead inexorably to the conclusion that there can be no reasonable expectation of privacy in that place."[24] Although one's right of privacy in public space must give way to the rights of other participants in that same space to observe what goes on around them, it by no means follows that one's right of privacy must give way with respect to data collected and recorded by public and private sector actors for a variety of specific purposes. Further, consent to the collection of discrete data particles is not necessarily consent to their matching and mining, or their transfer to other parties.[25]

Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril (Markham, Ont.: Butterworths, 2005) at 34-35, also echoes concerns that encroachments on privacy in public space may diminish expectations of privacy, although he argues that they should not automatically do so.

21 This view is reflected in the reasons of Justice Bastarache in *R. v. Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456 (S.C.C.), [*Kang-Brown*]. It is also explored in greater detail in Cohen, *ibid.*; See also Jennifer Chandler, "Privacy Versus National Security: Clarifying the Trade-Off" in Ian Kerr *et al.*, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford: Oxford University Press, 2009) at 5–22, online: On the Identity Trail <http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_Kerr_07.pdf>.

22 James A.Q. Stringham, "Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core for Section 8?" (2005) 23 C.R. (6^{th}) 245 at 251; Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) at 35, also discusses the social impact of the normalization of surveillance.

23 *R. v. Patrick*, 2009 SCC 17 (S.C.C.) [*Patrick*]; *Tessling*, *supra* note 17.

24 Cohen, *supra* note 20 at 34-35.

25 Data protection legislation makes it clear that consent must be obtained for the collection of data for specified purposes. Separate consent is required if the data is later to be used for other purposes. See e.g. *PIPEDA*, *supra* note 11, Sch. 1, cl. 4.3.1; *Personal Information Protection Act*, S.B.C. 2003, c. 63, ss. 7, 10 [*PIPA* (B.C.)]; *Personal Information Protection Act*, S.A. 2003, c. P-6.5, ss. 7, 13 [*PIPA* (Alberta)].

In *Aubry v. Les Éditions Vice-Versa inc.*,[26] the Supreme Court of Canada noted that, while persons photographed in public places generally have no basis for complaint about the publication of the photo in the media, this was only if their inclusion in the photo was incidental. The Court stated: "the public nature of the place where a photograph was taken is irrelevant if the place was simply used as a background for one or more persons who constitute the true subject of the photograph."[27] In a recent decision involving a civil action for invasion of privacy, Justice Soldevila of the Quebec Superior Court stated:

> . . . une personne demeure dans le cadre de sa vie privée lorsqu'elle est sur sa propriété, circule dans la rue et vaque à ses occupations habituelles, même si elle le fait à la vue de tous. Elle conserve donc en tout temps le droit de ne pas être observée et suivie systématiquement.[28]

In both *Aubry* and *Tremblay*, the context changes once an individual's presence or movements in public space become the focus of specific attention.[29]

(a) Characterizing the Privacy Interest

The context-sensitive nature of the reasonable expectation of privacy has pushed courts to develop a framework for determining what makes an expectation of privacy reasonable. An early approach saw Canadian courts divide privacy interests into three categories: personal, territorial and informational.[30] An individual's reasonable expectation of privacy varied depending on the classification of the privacy interest.

Personal privacy reflects the right an individual has to control over their physical person, and as such, is given a high level of protection by the courts.[31] "Personal" in this context is not a synonym for "private", but refers to one's physical person. Personal privacy "protects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal."[32] The right to personal privacy protects against unreasonable searches of one's body, the taking of blood or tissue samples, and other physically invasive searches.

However, territorial or spatial privacy recognizes an individual's privacy interests in a particular geographical space. For example, a person has a strong privacy

---

26 *Aubry c. Éditions Vice Versa Inc.*, 1998 CarswellQue 4806, *(*sub nom. *Aubry v. Éditions Vice-Versa inc.)* [1998] 1 S.C.R. 591 (S.C.C.) [*Aubry*].

27 *Ibid.* at para. 59.

28 *Tremblay c. Cie d'assurances Standard Life*, [2008] J.Q. No. 5252, 2008 QCCS 2488, 2008 CarswellQue 5339 (Que. S.C.) at para 59 [*Tremblay*].

29 Uteck considers this to flow from a loss of the anonymity that typically characterizes one's activities in public space. *Supra*, note 2 at 93.

30 See e.g. *R. v. Dyment*, [1988] 2 S.C.R. 417, ¶19-20 (S.C.C.) [Dyment]. These divisions are not absolute. In *Patrick*, *supra* note 23 at para. 26, the Supreme Court of Canada cautions that personal, territorial and informational privacy interests may frequently overlap.

31 See e.g. *R. v. Phoretsky*, [1987] 1 S.C.R. 945 (S.C.C.).

32 *Tessling*, *supra* note 17 at para 21.

interest in their home, as it is "the place where our most intimate and private activities are most likely to take place."[33] While apartment-dwellers will have a privacy interest in their apartments, a home owner's privacy interest extends to the surrounding land owned by her.[34] Spaces other than the home that have privacy significance may also be given some protection. Such spaces might include one's car,[35] a hotel room,[36] a rented locker,[37] or even spaces occupied by one's belongings such as a purse or backpack.[38]

Territorial privacy only protects a particular space as it relates to an individual. In other words, privacy "protects people not places."[39] Even though territorial privacy case law identifies and assesses the reasonable expectation of privacy in the context of a particular space, the existence, or location of that space is not inherently private. What takes place within one's home may be considered highly private, but the location of one's home — the street address — is information in the public domain. Location information as such is not typically protected by notions of territorial privacy. It is considered to have privacy dimensions only to the extent that it is personal information and, hence, it is typically considered under an "informational privacy" analysis.[40]

"Informational privacy" reflects one's privacy interests "[b]eyond our bodies and the places where we live and work."[41] Although physically unbounded, "information" about oneself and the ability to control it is central to dignity and integrity

---

33 *Ibid.* at para. 22.

34 See discussion of Binnie J. in *Tessling*, *ibid.* at para. 22; See also *R. v. Kokesch*, [1990] 3 S.C.R. 3 at 17-18 (S.C.C.); *R. v. Grant*, [1993] 3 S.C.R. 223 at 237 (S.C.C.); *R. v. Wiley*, [1993] 3 S.C.R. 263 at 273 (S.C.C.).

35 *R. v. Belnavis*, [1997] 3 S.C.R. 341 (S.C.C.) [*Belnavis*].

36 *R. v. Wong*, [1990] 3 S.C.R. 36 (S.C.C.).

37 *R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631 (S.C.C.).

38 *Tessling*, *supra* note 17 at 68; per Binnie J. Territorial privacy protection does not necessarily extend to spaces occupied by virtue of relationships, however intimate, such as the car of a close friend (*Belnavis*, *supra* note 35 at paras. 22-23); or a girlfriend's apartment (*R. v. Edwards*, [1996] 1 S.C.R. 128 (S.C.C.) [*Edwards*]).

39 *Patrick*, *supra* note 23 at para. 14 citing *Katz v. U.S.*, 389 U.S. 347 at 351 (U.S. S.C., 1967). For a critique of this concept, see Uteck, *supra* note 2 at 101.

40 Uteck, *supra* note 2, is critical of an approach that ignores the spatial privacy dimensions of location information. Certainly, when one compares the court of appeal (*R. v. Tessling* (2003), [2003] O.J. No. 186, 63 O.R. (3d) 1, 2003 CarswellOnt 181 (Ont. C.A.); leave to appeal allowed (2003), 2003 CarswellOnt 5831 (S.C.C.); reversed (2004), 2004 CarswellOnt 4351 (S.C.C.)) and Supreme Court of Canada decisions in *Tessling*, *supra* note 12, one can see the difference that a spatial privacy analysis can make to the outcome. This contrast is evident as well between the dissenting opinion at the Alberta Court of Appeal in *Patrick* (*R. v. Patrick*, 2007 ABCA 308 (Alta. C.A.); affirmed (2009), 2009 CarswellAlta 481 (S.C.C.)) and the Supreme Court of Canada's decision; Patrick, *supra* note 23. However, in the context of this paper, it is difficult to escape the informational privacy dimensions of location information, particularly in regard to its relationship with data protection legislation.

41 *Tessling*, *supra* note 17 at para. 23.

of the person.[42] Informational privacy raises "the thorny question of how much *information* about ourselves and [our] activities we are entitled to shield from the curious eyes of the state."[43] The nature and level of the informational privacy interest is very data and context specific. For some time, Canadian courts have focused on giving the highest level of protection to a "biographical core of personal information",[44] according little weight to other forms of personal information. This biographical core of information was described in *R. v. Plant*[45] as being information "which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[46] This concept has proven unwieldy, as it has involved courts passing judgment on what information "tends to reveal" details, and what details relate to "lifestyle and personal choices."[47] In critiquing this formulation as essentially circular, Pomerance writes: "[the courts] tell us that s. 8 will only protect the privacy of information if the information is inherently private."[48] In *R. v. M. (A.)*,[49] Justice Binnie cautioned against making decisions about privacy based on the categorization of the information at issue. He wrote:

> In *Dyment*, *Plant* and *Tessling*, the various categories of "information" (including "biographical core of personal information") were used as a useful analytical tool, not a classification intended to be conclusive of the analysis of information privacy. Not all information that fails to meet the "biographical core of personal information" test is thereby open to the police."[50]

This statement counters a trend towards a more restricted view of the kind of information in which one has a privacy interest.[51] Because of the growing ease

---

42 *Dyment*, *supra* note 30 at para. 22.

43 *Ibid.*

44 This phrase surfaced in *R. v. Plant*, [1993] 3 S.C.R. 281 at 293 (S.C.C.) [*Plant*].

45 *Ibid.*

46 *Ibid.* at 293.

47 In *Tessling*, *supra* note 17 at para. 26; Justice Binnie noted that this statement relating to "lifestyle and personal choices" was not meant to be exhaustive of the kind of information that would be protected, however, this did become a focal point for many courts.

48 Renée M. Pomerance, "Shedding Light on the Nature of Heat: Defining Privacy in the Wake of R. v. Tessling" (2005) 23 C.R. (6th) 229 at 233.

49 *R. v. M. (A.)*, 2008 CarswellOnt 2257, 2008 SCC 19, 55 C.R. (6th) 314 (S.C.C.).

50 *Ibid.* at para. 68.

51 This approach is evident in a number of cases. For example, in *R. v. Wilson* (February 10, 2009), Court File No.: 4191/08 (Ont. S.C.) [*Wilson*]; Leitch J. of the Ontario Superior Court found that there was no expectation of privacy in an internet subscriber's name and address, even though in the case, the police were interested in this data because it was the key to linking an individual to certain internet-based activities. Leitch J. rejected the finding of Gorewich J. in a similar case that linking subscriber information with internet activities did in fact amount to information that would "tend to disclose intimate details of lifestyle and activities" — *R. v. Kwok* (2008), [2008] O.J. No. 2414, 2008 CarswellOnt 2634, ¶35 (Ont. C.J.) [*Kwok*]; In *R. v. Vasic* (2009), [2009]

with which apparently innocuous information can be linked to and matched with other data, a more flexible approach to assessing the privacy interest in information is warranted. A single piece of information can convert anonymous data into highly sensitive personal information about identifiable individuals.[52] In *Tessling*, Binnie J. acknowledged that advances in technology could change the nature and quantity of information being gathered, thus, requiring departures from earlier case law.[53]

In *Tessling*, the heat signature data gathered by the police using aerial Forward Looking Infrared (FLIR) technology merely measured the heat emanating from a house. The court ruled that this was not core biographical information.[54] As a result, the gathering of the information, which took place without physical intrusion, did not violate *Charter* rights to privacy, notwithstanding the fact that technology was needed to obtain and record it. Location information about an individual is less likely to be treated in this manner, as it is directly generated by the actions and choices of an individual. In other words, it conveys a direct message about where an individual was at a particular point in time, which in turn tells us something about that individual's choices and activities. The greater risk with location information is that it will be considered as a simple proxy for what was easily and readily observable at the time. In other words, if a person had no reasonable expectation of privacy in their passage from one point in the city to another, using city streets, then what expectation of privacy would they have in data that simply recorded this transit?

O.J. No. 685, 2009 CarswellOnt 846 (Ont. S.C.J.) [*Vasic*], Thorburn J. also accepted that providing account information to someone in possession of an IP address might result in access to core biographical data. These cases are discussed in more detail below.

52 See e.g. *Wilson*, *ibid.* This point is also made in the access to information context in *Gordon v. Canada (Minister of Health)*, 2008 FC 258, 324 F.T.R. 94 (F.C.). It should be noted that the significance of this issue may be ignored by courts in some cases. For example, in *R. v. Ward* (2008), [2008] O.J. No. 3116, 2008 CarswellOnt 4728 (Ont. C.J.) [*Ward*], the court notes that an internet protocol (IP) address is a piece of information that conveys nothing significant about an individual. This is only true in the abstract. If the IP address is the key to linking a variety of internet activities to that individual, then the IP address becomes a very significant piece of information.

53 *Tessling*, *supra* note 17 at paras. 25–29; In *R. v. Mahmood* (2008), [2008] O.J. No. 3922, 79 W.C.B. (2d) 366, 2008 CarswellOnt 5907 (Ont. S.C.J.); additional reasons at (2009), 2009 CarswellOnt 4520, ¶65 (Ont. S.C.J.) [*Mahmood*], the court echoes this in noting the need for analytical flexibility as technology advances.

54 This decision has been widely criticized. See e.g. Ian Kerr & Jena McGill, "Emanations, Snoop Dogs and Reasonable Expectations of Privacy", (2007) 52 Crim. L.Q. 392 at 431, online: On the Identity Trail <http://www.idtrail.org/files/kerr_mcgill_-_emanations_snoop_dogs_and_reasonable_expectations_of_priva.pdf>; See also Pomerance, *supra* note 48; Stringham, *supra* note 22; Steve Coughlan & Marc S. Gorbet, "Nothing Plus Nothing Equals . . . Something? A Proposal for FLIR Warrants on Reasonable Suspicion" (2005) 23 C.R. (6^{th}) 239.

(b) The Contextualized Approach

In *Tessling*, the Supreme Court of Canada offered a framework for assessing the existence of a reasonable expectation of privacy in the information privacy context.[55] Justice Binnie drew this test from *R. v. Edwards*,[56] an earlier decision of that Court which dealt with an issue of territorial or spatial privacy. The migration of the test to the context of an informational privacy case suggests a more unified approach that regards the nature of the privacy interest in a broader context. The *Tessling* approach first considers whether the individual had a subjective expectation of privacy in the information gathered, and then asks whether that expectation was objectively reasonable. In order to assess the objective reasonableness of the expectation, the Court identified the following factors for consideration:

a) the place where the alleged "search" occurred;

b) whether the subject matter was in public view;

c) whether the subject matter had been abandoned;

d) whether the information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality?

e) whether the police technique was intrusive in relation to the privacy interest;

f) whether the use of surveillance technology was itself objectively unreasonable;

g) whether the [technology used] exposed any intimate details of the respondent's lifestyle, or information of a biographical nature.[57]

The first consideration indicates that location may be relevant — it incorporates a territorial privacy dimension to the analysis. The second relates to the visibility of the item or activity. Both considerations suggest that there may be little or no expectation of privacy in things that may be readily observed.

Activities that may be observed by anyone in the general vicinity would certainly fall within the category of things in public view.[58] It is less clear that recorded information — such as that captured by video cameras — is information "in public view."[59] There are many who would argue that such activity is necessarily in public view, and that there is no reasonable expectation of privacy where cam-

---

55 This framework is reaffirmed in *Patrick*, *supra* note 23 at paras. 26-27.

56 *Edwards*, *supra* note 38.

57 *Tessling*, *supra* note 17 at para. 32.

58 In the U.S., for example, there is case law to the effect that a warrant is not needed for police to place a tracking device on a car, as this device will only track movements otherwise open to public observation. *U.S. v. Knotts*, 480 U.S. 276 (1983) (regarding a tracking device on a container carried in a vehicle); See also *U.S. v. Karo*, 468 U.S. 705 (1984); *U.S. v. Garcia*, 474 F. 3d 994 (7th Cir. 2007). The situation is otherwise in Canada — see *R. v. Wise*, [1992] 1 S.C.R. 527 (S.C.C.).

59 Indeed, Lai argues that public video surveillance engages s. 8 of the *Charter* — see Derek Lai, "Public Video Surveillance by the State: Policy, Privacy Legislation, and the *Charter*" (2007) 45 Alta L. Rev. 43.

eras in public spaces record the activities of passers-by.[60] The use of surveillance cameras in public spaces is often justified on the basis that these cameras only record events otherwise open to public view. It is argued that if a person is in public view, she cannot prevent others from observing her activities, mannerisms, clothing or companions.[61] Some would even go so far as to say that the widespread use of video cameras in public spaces drastically reduces the reasonableness of any expectation of privacy, as people realize that they may be under observation at any time and in virtually any public place.[62]

Recorded location information is of a different character from observations of individuals in public space. To begin with, the quality of the information is frequently richer than casual observation. For example, while the use of a cell phone on a city street may reveal that the caller (or recipient of a call) was in a particular geographic area at a specific point in time, the fact that this could also have been observed by others who were in that precise area at the time, and who happened to notice the person using their phone, does not mean that the recorded data is merely a representation of what was in public view. The recorded data will also reveal the identities of the caller and of the recipient of the call, and this information goes well beyond what could be observable by bystanders. As surveillance camera technology continues its rapid evolution, individuals captured in images may also become identifiable in ways that would not be possible through mere observation by bystanders or even by human surveillance agents. Recorded data is of an entirely different character from human observation, and the advancing technology for refining, matching and sorting this data makes it even more so.[63]

---

60 *U.S. v. Vazquez*, 31 F. Supp. 2d 85 at 88 (D. Conn. 1998).

61 Indeed, this is the argument used in the private sector context by Google to rebuff claims that Street View is privacy invasive. See e.g. "Street View will comply with Canada's privacy laws: Google" *CBC News* (25 September 2007), online: CBC <http://www.cbc.ca/technology/story/2007/09/25/tech-google-streetview.html>.

62 See e.g. David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity Press, 2007) at 176. However, Lai suggests that in the Canadian context, it is not a foregone conclusion that courts will flatly reject a reasonable expectation of privacy in public spaces — Lai, *supra* note 59 at 67. Nevertheless, the Supreme Court of Canada was certainly deeply split (in *Kang-Brown*, *supra* note 21) over the appropriate threshold (reasonable and probable grounds or reasonable suspicion) that would trigger the ability of police to use sniffer dogs in a public bus terminal. Similarly, Paton-Simpson notes that the emerging law around the tort of invasion of privacy seems to go both ways on the issue (Paton-Simpson, *supra* note 15 at 314–316). Still, there are indications that the law of Quebec, at least, favours some degree of privacy in public space. See *Aubry*, *supra* note 26; See also *Tremblay*, *supra* note 28.

63 See e.g. David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies" in Lyon, *ibid.* at 13–30; Lai, *supra* note 59 at 51; Kevin D. Haggerty & Richard V. Ericson, "*The New Politics of Surveillance and Visibility*" in Kevin D. Haggerty & Richard V. Ericson, eds., The New Politics of Surveillance and Visibility (Toronto: University of Toronto Press, 2007) 3–25 at 5; Uteck, *supra* note 2 at 88–91, also discusses the impact that ubiquitous computing will have on the nature, quality and volume of location information that it will generate.

Further, the *capture* of this location information changes its character from a simple observation to a *record*, which in turn raises its own privacy implications. A record is more tangible and concrete than an observation, it may also be more precise, more enduring, more easily located, matched and mined. The number and character of potential viewers of the recording may change dramatically. Recorded acts also achieve a relative level of permanence, and this record alters their significance and consequences. Passing through public view is quite different from being recorded in public view.[64]

Thus, at the point at which information about one's activities has been recorded by a private sector actor, the information at issue is no longer a simple observation. As Bennett and Crowe note, there is "an important distinction between the routine capture of personal data and the subsequent analysis of that data for the purposes of making a decision about that person."[65] Indeed, this is recognized by the fourth factor in the *Tessling* analysis — whether the information was in the hands of a third party.

II. DATA IN THE HANDS OF THIRD PARTIES

In Canada, the applicability of data protection legislation in the private sector creates an additional and important layer to the analysis of the reasonable expectation of privacy in location data. Data protection legislation operates within a consent-based paradigm, where one is considered to have expressly or impliedly consented to the collection of the data under certain terms and conditions. Those terms and conditions may outline whether, and under what conditions, the data may be shared with agents of the state. In addition, specific provisions of data protection statutes may also permit the sharing of this data with law enforcement officials without the data subject's consent.

In an environment where private sector actors are in a position to collect and compile a rich body of data that tracks our movements and activities, it is crucial to understand the relationship between data protection legislation and one's reasonable expectation of privacy regarding the information collected about one. This issue has exploded in the internet context, with a series of cases dealing with the exceptions for disclosure of information without consent to law enforcement officials

---

64 Colin Bennett, Charles Raab & Priscilla Regan, "People and Place: Patterns of individual identification within intelligent transportation systems" in David Lyon, ed., *Surveillance as Social Sorting: Privacy Risk and Digital Discrimination* (N.Y.: Routledge, 2005) 151–175 at 157. Bennett et al make the point that the public nature of the activity of driving changes its character when ITS is used to collect and record extensive data about individual drivers. See also Reg Whitaker, "A Faustian Bargain? America and the Dream of Total Information Awareness" in Kevin D. Haggerty & Richard V. Ericson, eds., *The New Politics of Surveillance and Visibility* (Toronto: University of Toronto Press, 2007) 141 at 141-142.

65 Colin J. Bennett & Lori Crowe, "Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada", Report to the Office of the Privacy Commissioner of Canada (June 2005) at 8, online: University of Victoria <http://web.uvic.ca/polisci/bennett/pdf/lbsfinal.pdf>.

under PIPEDA.[66] It has also received media attention in the context of the *Technical Assistance for Law Enforcement Act* (BILL C-47), a Bill that is currently before Parliament.[67]

One of the contextual factors in the *Tessling* analysis is "whether the information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality?" There are two threads here. The first suggests that there is a lower expectation of privacy in information that has already "escaped" from the control of the individual and is in the hands of a third party. The second is that an expectation of privacy may survive this "escape" if the third party owes an obligation of confidence to the individual.[68]

Location data is typically collected and recorded either by a public or a private sector entity and, thus, is usually in the hands of a third party. Data protection legislation imposes legal obligations on those who collect, use and disclose personal information, and may place strict limits on the situations in which information may be disclosed to others without the data subject's consent. In the case of location information, PIPEDA is particularly important, as it will apply to data in the hands of telecommunications organizations such as internet service providers and cell phone companies.[69] In a world of mobile communications, these service providers will increasingly gather detailed location information about their clients. Depending upon the circumstances, PIPEDA's provisions will also apply to a wide range of other organizations that collect, use or disclose personal information in the course of commercial activity.

These situations — where location information or other personal data is sought by government from private sector third parties — sit on the cusp between data protection legislation (which governs the collection, use or disclosure of personal information by private sector entities) and the *Charter* (which balances privacy interests with the interests of the state). If data protection legislation gives an open-ended discretion to companies to disclose personal information to police without the data subject's consent, and without need for judicial authorization, a person's reasonable expectation of privacy in this information would certainly seem to be diminished.[70]

This tension between a reasonable expectation of privacy and data protection law is evident in recent case law. There have been a series of court decisions in-

---

66 *PIPEDA*, *supra* note 11.

67 Bill C-47, *supra* note 13.

68 In analyzing the decision of the Ontario Court of Appeal in *Tessling*, Lisa M. Austin, "One Step Forward or Two Steps Back? *R. v. Tessling* and the Privacy Consequences for Information Held by Third Parties" (2004-05) 49 Crim. L.Q. 22, critiques an approach to information privacy that assumes a loss of a privacy interest once one's personal information is in the hands of a third party.

69 Where a service provider is a provincial crown corporation, it is possible that provincial legislation may apply. See *R. v. Trapp*, 2009 SKPC 5, [2009] S.J. No. 32, 2009 CarswellSask 48 (Sask. Prov. Ct.) [*Trapp*].

70 Nouwt, *supra* note 3 at 397-398; also writes about the risks to privacy that arise if collections of private sector location data become too easily accessible to law enforcement officials.

volving s. 8 *Charter* challenges to the way in which police obtained customer information from internet service providers (ISPs), which they then linked to IP addresses associated with online child pornography-related activities. The cases raise a cluster of inter-related issues, including: the meaning to be given to "lawful authority" in s. 7(3)(c.1) of PIPEDA, the relevance of a privacy policy to the determination of the reasonable expectation of privacy, and the possibility that a reasonable expectation of privacy may exist *vis à vis* the state with respect to some information regardless of the terms of the privacy policy or the language of the relevant data protection statute.

Data protection legislation sets normative boundaries for the collection, use and disclosure of personal information. Such legislation is generally premised on consent-based models, and it is usual for the terms and conditions for collection, use and disclosure of personal information to be set out in privacy policies linked to consumer contracts. PIPEDA, along with its substantially similar provincial counterparts,[71] provides limited exceptions for disclosures of personal information without consent. For example, PIPEDA contains a specific provision addressing the disclosure of personal information held by an organization for law enforcement purposes:

> 7(3) . . . an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
>
> . . . .
>
> (c.1) made to a government institution or part of a government institution that has made a request for the information, *identified its lawful authority to obtain the information and indicated that*
>
> (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
>
> (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
>
> (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

The interpretation of this provision has been a matter of some recent controversy. Disclosure without consent may be made to a government institution where it has "identified its lawful authority to obtain the information." If "lawful authority" means a court order or search warrant, then clearly this sort of information, sought for the purposes of law enforcement or national security, may only be disclosed without the consent of the data subject where such a warrant or order is obtained. However, it is not clear whether "lawful authority" means either judicial authorization, or perhaps specific statutory authority granted under a relevant stat-

71 *Supra* note 25.

ute.[72] Some courts have indicated that a police officer's "lawful authority" might simply be his or her status as an agent of the state carrying out an investigation.[73]

The interpretation to be given to this provision is important in that it creates an avenue through which data in the hands of third party organizations can be accessed by law enforcement with few checks and balances. The blurring between information gathering by the state and information gathering by the private sector is a matter of concern that has been raised by the Privacy Commissioner of Canada. In an appearance before the Standing Committee on Access to Information, Privacy and Ethics Commissioner Stoddart stated:

> [W]e're also concerned about the increasing blurring of the lines between the private sector and the public sector. In Canada, we're used to the state carrying out laws, certainly carrying out criminal law and national security issues. With a change to PIPEDA that came about two years ago, organizations in Canada are now mandated to specifically request information, to collect it for the express purpose of giving it to the national security authority.[74]

Commissioner Stoddart was referring to the amendment to PIPEDA which added s. 7(1)(e), which permits organizations to gather information without consent for the purposes of handing it over to national security officials.[75] This is distinct from s. 7(3)(c.1) in that it involves pro-active data gathering, and may turn the data collector into an agent of the state whose activities would be subject to review under s. 8 of the Charter.[76] Nevertheless, there is still a blurring of the lines between public and private with disclosure of personal information under s. 7(3)(c.1) to the extent that there is a vast store of personal information that is potentially open to the scrutiny of state authorities. The terms under which these agents of the state may gain access are crucially important to individual privacy.

(a) The Cases

As noted earlier, there has been a flurry of case law dealing with the interpretation of s. 7(3)(c.1) in relation to internet subscriber information. These cases involve investigations relating to child pornography, and reflect a context in which there is a strong motivation to see the perpetrators brought to justice. Yet, the issues raised in these cases are not exclusive to that context. Section 7(3)(c.1) potentially enables a flow of personal information between private sector companies and law enforcement officials across a broad range of law enforcement issues. In the discus-

---

72 See e.g. *Income Tax Act*, R.S.C. 1985, c. 1 (5th Supp.), s. 231.2. These provisions permit officials to have access to certain records in specified circumstances.

73 See e.g. *Wilson*, *supra* note 51; *Vasic*, *supra* note 51.

74 *Standing Committee on Access to Information, Privacy and Ethics*, 39th Parl., 1st Sess., No. 003 (5 June 2006) at 1539.

75 Section 7 of PIPEDA was amended by the *Public Safety Act*, 2004, c. 15, s. 98. In the U.S. context, the actions of some large private sector companies post 9–11 in turning over large volumes of consumer data to law enforcement officials raised substantial concerns about privacy in that country. See Robert O'Harrow Jr., *No Place to Hide* (New York: Free Press, 2005); Whitaker, *supra* note 64.

76 Israel *et al.*, *supra* note 8 at 11.

sion below, the three main issues considered by the courts will be addressed. These are 1) the meaning of "lawful authority" in s. 7(3)(c.1) of PIPEDA; 2) the significance of the terms of privacy policies; and 3) whether there is a reasonable expectation of privacy in the information at issue.

(i) Interpreting "Lawful Authority"

A number of Canadian cases have considered whether "lawful authority" in PIPEDA means judicial authorization, or whether it can simply mean identifying the credentials of the requestor. In *C. (S.), Re*,[77] a child pornography case, police used a "Letter of Request" to obtain subscriber data from the accuseds' ISP. The court described this request as having been made "under the authority of P.I.P.E.D.A.."[78] In considering the meaning of "lawful authority", Conacher J. found that the existence of a criminal investigation was not, on its own, "lawful authority."[79]

In *R. v. Kwok*,[80] police sought subscriber information to match with an IP address linked to child pornography-related activities on the internet. The Internet Service Provider (ISP) provided the information to police on request, without judicial authorization. It was argued that this violated the s. 8 rights of the accused. In considering the *Charter* issues, Justice Gorewich took into account the role of PIPEDA in creating a reasonable expectation of privacy in the data in the hands of the ISP. He observed that prior to PIPEDA, officers regularly used warrants to obtain the type of information at issue in the case. Thus, one of the issues was whether PIPEDA altered that *status quo* by removing the requirement to obtain a warrant. Justice Gorewich noted that s. 7(3)(c.1) of PIPEDA requires a requesting party to identify its lawful authority to obtain the desired information. That party must also indicate that the information is required for the purpose of enforcing a law of Canada. He found that it is reasonable to find that "lawful authority" can include a person's authority as a police officer. He stated "[g]iven the stated purpose of the Act, and in particular s. 7(3)(c), to hold it means only a warrant does not make any logical sense."[81]

In *R. v. Mahmood*[82] the court considered the legality of a series of warrants issued for the dump of a significant volume of call data from cell phone towers based on the geographic location of the calls. The case does not resolve the "lawful authority" question because the warrants obtained by police were ruled invalid and, therefore, could not constitute "lawful authority" to obtain the data. However, Justice Quigley does express support for the view that "lawful authority" means judi-

---

77 *C. (S.), Re*, 2006 CarswellOnt 5732, 2006 ONCJ 343 (Ont. C.J.) [*C. (S.), Re*].

78 *Ibid.* at para. 3.

79 *Ibid.* at para. 9.

80 *Kwok*, *supra* note 51.

81 *Ibid.* at para. 32. Section 7(3)(c) permits disclosure without consent to comply with a subpoena or warrant.

82 *Mahmood*, *supra* note 53.

cial authorization. This expectation of privacy is further bolstered by PIPEDA.[83] Justice Quigley writes:

> Clearly PIPEDA requires that a police authority seeking personal information, such as that disclosed in both the Tower Dump Records and the Subscriber Records, provide the cellular phone service provider with either a subpoena or warrant issued by a court or other authorized person or body. Alternatively, at a minimum, if it actually entails a lesser standard (which to my mind is not immediately evident), a governmental authority seeking such information must have identified its lawful authority to obtain the information and indicated it is required for purposes of law enforcement or in furtherance of an investigation.[84]

Justice Quigley stops short of categorically stating that "lawful authority" means judicial authorization. In doing so, he suggests that there might be some circumstances where something less than a warrant (and perhaps not much more than a police officer identifying herself and stating she is investigating a crime) would be required.

The interpretation of s. 7(3)(c.1) of PIPEDA may also be affected by the overarching reasonableness principle in s. 5(3) of PIPEDA. This section provides that: "An organization may . . . disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." The permission to disclose without consent in s. 7(3)(c.1) may be limited by s. 5(3) to disclosure only where a reasonable person would consider it appropriate to disclose the information without a warrant.[85] If this is the case, then the issues of the terms of any privacy policy and the general privacy interest in the information at issue are highly relevant.

(ii) The Significance of Privacy Policies

In *R. v. Ward*,[86] another internet child pornography case, the court found that there was no reasonable expectation of privacy in customer data held by an ISP. The data had been provided to the police by the ISP in response to a written request that was not supported by judicial authorization. The terms of the company's privacy policy, incorporated by reference into the customer contract, provided that customer data would not be released to police without "lawful authority" — language similar to that used in s. 7(3)(c.1) of PIPEDA. Justice Lalande interpreted this to mean that the customer had no reasonable expectation of privacy in the data *vis à vis* law enforcement agents presenting lawful authority. Unfortunately, his analysis avoided interpreting "lawful authority." If "lawful authority" means judicial authorization, then customers do have an expectation that their personal data will not be turned over unless a search warrant is presented. On the other hand, if

---

83 Quigley J. cites *BMG Canada Inc. v. John Doe*, [2004] 3 F.C.R. 241 (F.C.); affirmed (2005), 2005 CarswellNat 1300 (F.C.A.) on this point.

84 *Mahmood*, *supra* note 53 at para. 74.

85 For a discussion of the normative impact of s. 5(3), see Lisa M. Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA" (2006) 56 U.T.L.J. 181.

86 *Ward*, *supra* note 52.

"lawful authority" simply means that a police officer need only identify herself as a police officer investigating a crime, then it would be more appropriate to conclude that a customer has very little, if any, expectation of privacy in their information *vis à vis* state authorities.

The reliance on a privacy policy to find that there is no reasonable expectation of privacy is apparent in other cases as well. For example, in *R. v. Wilson*,[87] Justice Leitch was also faced with a *Charter* claim by an accused charged with child pornography related charges. The police had used a letter to the ISP to obtain customer data that ultimately linked the accused with the offending internet activities. The "lawful authority" asserted in the request was the status of the requester as a police officer. Justice Leitch endorsed the approach that examined the privacy policy of the ISP in *Ward*. In this case, the subscriber agreement indicated that the ISP would disclose personal information without knowledge or consent in order to comply with a subpoena or court order, or "as may be otherwise required by law." In her view, this negated any reasonable expectation of privacy in the information. However, as in *Ward*, it is not clear how that language actually indicates that information will be disclosed without a subpoena or warrant, merely on the permissive language of s. 7(3)(c.1). After all, s. 7(3)(c.1) does not actually require the disclosure of information without consent.

In *Mahmood*,[88] which considers the reasonable expectation of privacy in location data outside the internet context, the court found that the contracts between cell phone providers and their clients, backed by data protection legislation, created a reasonable expectation of privacy in this data. In the view of Justice Quigley, this expectation was very much a product of the existence of data protection legislation, which set clear limits on the collection, use and disclosure of personal information.[89] Quigley J. noted that the various cell phone contracts incorporated by reference the companies' privacy policies. These privacy policies indicated that personal information would not be provided to the authorities without "lawful authority." Quigley J. found that "[t]his gave them a legitimate and reasonable objective expectation of privacy in the records provided to the police by the cell phone service providers."[90]

In *R. v. Vasic*,[91] the court also considered the role of the service contract in determining the reasonable expectation of privacy. The Account Holder Agreement with the ISP, Rogers, stated that "all information kept by Rogers regarding you, as the account holder, *other than your name, address and listed telephone number*, is confidential and may not be disclosed by Rogers to anyone other than you."[92] For Justice Thorburn, the express exclusion of the name, address and telephone number from the list of information that Rogers undertook to keep confidential meant that the subscriber could have no reasonable expectation of privacy in the information.

---

87 *Wilson*, *supra* note 51.

88 *Mahmood*, *supra* note 53.

89 *Ibid.* at para. 56.

90 *Ibid.*, at para. 73.

91 *Vasic*, *supra* note 51.

92 This extract is cited in *Vasic*, *ibid.* at para. 11. The emphasis is added by the Court.

It would appear that data protection legislation does play a role in determining the reasonable expectation of privacy an individual may have in their personal information in the hands of the police. Section 7(3)(c.1) is not determinative of the issue — it is permissive in nature. Courts clearly look to the terms of any service agreement or privacy policy between the service provider and the data subject. Unfortunately, these terms have not always been entirely clear, and courts have, thus far, not been generous towards the expectations of data subjects in interpreting them. It is important to keep in mind, however, that in the majority of these cases, the data sought has been in the hands of ISPs.

In both *Vasic* and *Ward* the courts were prepared to find that any reasonable expectation of privacy could be negated by the existence of a customer agreement that permitted disclosure of the information to law enforcement without knowledge or consent of the customer. Yet, it should not be so readily assumed that a customer agreement or privacy policy can be taken automatically to obliterate a reasonable expectation of privacy in data in the hands of third parties. Many such polices are not read by consumers for a variety of reasons.[93] It may be artificial to find that a person's expectation of privacy in data they did not realize was being collected or retained is governed by an agreement of which they were largely unaware. As Pomerance notes,

> [p]ersonal data is constantly acquired, stored and disseminated by government and private agencies. Information has often been sold or transferred without our permission or even knowledge. Even knowledge of such transfers does not necessarily imply a full appreciation of the consequences.[94]

Courts should take care to ensure that the data subject had proper notice of the terms of the policy. The obliteration of the reasonable expectation of privacy is more palatable in contexts where the service being provided (such as internet service) is one that can be used for either legal or illegal purposes. In such a context, subscribers are likely aware that their online activities may have repercussions. A party using the service for illegal purposes who does not inform himself of the service provider's reporting policies may be considered willfully blind to the terms of the agreement. In other contexts, where, for example, location data in the hands of third party companies is more incidental to the goods or services provided, it may be less appropriate to tie the reasonableness of the data subject's expectation of privacy to the terms of a privacy policy. If the data is of a kind in which a reasonable expectation of privacy exists, it may not be constitutionally appropriate for law enforcement officials to seek it without judicial authorization.

---

93 For example, a recent study by the Canadian Internet Policy and Public Interest Clinic found that many privacy policies are very lengthy, and some require a reader to consult multiple documents (at 6). The same study found that many policies were difficult to understand (at 19). See Canadian Internet Policy and Public Interest Clinic, *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (April 2006), online: CIPPIC <http://www.cippic.ca/uploads/May1-06/PIPEDAComplianceReport.pdf>.

94 Pomerance, *supra* note 48 at 234.

Even if one accepts the view of some courts that the clear terms of a customer agreement can completely negate any expectation of privacy,[95] the wording of s. 5(3) — the overarching requirement that disclosure may only be for purposes that a reasonable person would consider are appropriate in the circumstances — may affect the analysis. If this is the case, then regardless of the terms of the agreement, the data subject may retain an expectation of privacy in the data that would prevent disclosure without judicial authorization. This would occur if the data is of a kind in which a strong and reasonable expectation of privacy would exist.[96] Of course, it is also open to consider that the reasonable person would consider it appropriate to disclose the information without consent where the individual has clearly agreed to these terms. However, notwithstanding a privacy policy that indicates that certain information may be disclosed to police without an individual's knowledge or consent, for example, it might not be reasonable for a third party data processor to respond to a request for data about a large number of individuals.

(iii) The Reasonable Expectation of Privacy in the Information at Issue

If a service contract is not to be relied upon, or if its wording is ambiguous, a further issue is whether a reasonable expectation of privacy exists in the information at issue. The issue may also arise where a privacy policy makes it clear that the company may, at its own discretion, disclose information to police pursuant to a police request and without judicial authorization. Such an analysis focuses on the nature of the information. This issue has been considered by the courts in the ISP cases. For example, in addition to finding that the service contract did away with any reasonable expectation of privacy, Justice Leitch in *Wilson* went further and found that the information in question — a subscriber's name and address — did not qualify as personal information in which there was a reasonable expectation of privacy.[97] She categorized it as "information available to anyone in a public directory and it does not reveal, to use the words of Sopinka J. in *Plant*, 'intimate details of the lifestyle and personal choices or decisions of the applicant.'"[98] In reaching this conclusion, she explicitly rejected the finding of Justice Gorewich in *R. v.*

---

95 See e.g. the decision in *Vasic*, *supra* note 51.

96 In this regard some of the recent cases have been very disappointing. In *Wilson*, *supra* note 51, for example, the court took the view that a name and address were not core biographical information and, thus, carried no reasonable expectation of privacy, notwithstanding the fact that this information was the key needed to unlock the "meaning" of the IP address in the hands of the police and, thus, to link online activities (in which a much greater expectation of privacy must surely exist) with the ISP subscriber. A similar disappointing conclusion was drawn in *R. v. Trapp*, *supra* note 69. However, the courts in *Kwok*, *supra* note 51; *Ward*, *supra* note 52; and *Vasic*, *supra* note 51, seemed to reach different conclusions.

97 This view appears to be supported in Israel *et al.*, *supra* note 8 at 17.

98 *Wilson*, *supra* note 51 at para. 51. This approach, which considers the customer data as having no privacy implications because it is public information, and which assesses it as an isolated, decontextualized piece of information, is precisely what is criticized as inappropriate in an information society by privacy theorist Helen Nissenbaum — Helen Nissenbaum, "Toward an Approach to Privacy in Public: Challenges of Information Technology" (1997) 7(3) Ethics & Behaviour 207.

Kwok that such information, because it is needed to link a person to an IP address associated with certain behavior on the internet, did in fact amount to information that "would tend to disclose intimate details of lifestyle and choices."[99]

In *R. v. Vasic*[100] Justice Thorburn was prepared to accept that "disclosure of the name and municipal address, to someone who possesses the IP address, may provide the holder of the IP address with 'details of the lifestyle and personal choices of the individual.'"[101] In *C. (S.), Re*, the court found that the subscriber information was information in which "a citizen would have an expectation, and a reasonable one, of privacy."[102] In the cell phone context, the court in *Mahmood* considered that the cell phone call data contained, at least in part, "some of the elements of biographical core", particularly "some general identification of movement, of personal associations, and of frequency of contact with associated persons."[103]

In *R. v. MacInnis*[104] Ferguson J. considered an application to exclude as evidence the cell phone records of the accused's common law wife. The accused, Knight, cohabited with his common law spouse, Larmand, and they had a child together. Each subscribed to a different cell phone service. There was evidence to show that during the period covered by the indictment, Knight frequently used Larmand's cell phone.

The court considered whether there was a privacy interest in cell phone usage data. Ferguson J. noted that a number of cases in Canada had held that a person

> has no privacy interest in the telephone number, subscriber information (such as their name, address, etc.) and even in the call detail information for cell phones which records the numbers called, the times and length of calls and the general location of their cell phone by reference to cell tower involvement.[105]

---

99 *Kwok*, *supra* note 51 at para. 35. This view of subscriber information has subsequently been endorsed, in the civil context in Ontario, in *Warman v. Wilkins-Fournier* (2009), [2009] O.J. No. 1305, 2009 CarswellOnt 1665 (Ont. S.C.J.). This case is currently on appeal to the Ontario Court of Appeal. The approach in *Warman* in characterizing the nature of the information is distinctly different from that of the Federal Court of Appeal in *BMG Canada Inc. v. John Doe*, 2005 FCA 193, [2005] 4 F.C.R. 81 (F.C.A.). In that case, the Court appears to accept that information about internet activities, when linked with a subscriber's identifying information could be "highly confidential" — *BMG*, *ibid.* at para 44.

100 *Vasic*, *supra* note 51.

101 *Ibid.* at para. 54, citing *Plant*, *supra* note 44.

102 *Supra* note 77 at para. 6.

103 *Ibid.* at para. 77.

104 *R. v. MacInnis* (2007), [2007] O.J. No. 2930, 2007 CarswellOnt 4770 (Ont. S.C.J.); *R. v. MacInnis* (2007), [2007] O.J. No. 2937, 2007 CarswellOnt 4817 (Ont. S.C.J.).

105 *Ibid.* at para. 32. The court referenced the Supreme Court of Canada's decision in *R. v. Plant*, *supra* note 44, noting that in *Plant*, the court indicated that "the focus should be on whether the records contain a biographical core of personal information which individuals in Canada would wish to keep private." *Plant*, *ibid.* at para. 35.

For example, the court cited the decision of the Alberta Court of Appeal in *R. v. Pervez*,[106] which found that the accused had no privacy interest in cell phone records because the records "do not reveal intimate details of Pervez's lifestyle or personal choices."[107] By contrast, in *R. v. Bryan*, the court found that cell phone billing information "has a confidential informational component readily distinguishable from the intrusion on privacy flowing from disclosure of hydro records."[108] In *R. v. Cole*,[109] the court was prepared to recognize only a fairly limited privacy interest in cell phone call data, stating: "[t]he accused's expectation of privacy in the cell phone records was low given the nature of the commercial records and their substance."[110]

In *MacInnis*, Ferguson J. distinguished earlier case law that found that there was generally no reasonable expectation of privacy in cell phone usage records on the basis that PIPEDA has now overtaken this case law, and had created a privacy interest in phone records. He stated: "[s]ince the information collected with respect to cell phone numbers relates to the subscriber, the Act creates an objective expectation of privacy for the subscriber."[111] He also noted that s. 492.2 had been added to the *Criminal Code*, providing a form of search warrant process "to justify the installation of number recorders which would capture some of the information available from cell phone providers."[112] In his view, this suggests that "parliament considered that individuals have a privacy interest in such information."[113] He concluded that "there is no doubt now that an individual telephone subscriber has a privacy interest in his or her own telephone data collected by a service provider."[114] He also extended this expectation of privacy to "some persons whose personal information is contained in the records relating to a subscriber."[115] He expressed the principle in these terms:

> If the cell phone is used by a person other than the subscriber, with the consent of the subscriber, then in my view the user has a reasonable, subjective expectation that the information will be kept confidential. The statutory duty to keep the information confidential creates an objective expectation of privacy for such users.[116]

It is not clear whether the conclusion by Ferguson J. that PIPEDA creates a reasonable expectation of privacy in cell phone call data is meant to survive the presence of a subscriber agreement or privacy policy that negates this expectation.

---

106 *R. v. Pervez* (2005), [2005] A.J. No. 708, 2005 CarswellAlta 810 (Alta. C.A.).

107 *Ibid.* at para. 12.

108 *R. v. Bryan* (1999), [1999] O.J. No. 5074, 1999 CarswellOnt 4787, ¶14 (Ont. S.C.J.).

109 *R. v. Cole* (2006), [2006] O.J. No. 1402, 60 W.C.B. (2d) 611, 2006 CarswellOnt 2157 (Ont. S.C.J.).

110 *Ibid.* at para. 32.

111 *Ibid.* at para. 44.

112 *Ibid.* at para. 45.

113 *Ibid.*

114 *Ibid.* at para. 46.

115 *Ibid.* at para. 48.

116 *Ibid.*

In *Kwok*, in spite of his finding that a warrant was not required by s. 7(3)(c.1) in all circumstances, Justice Gorewich went on to consider the privacy interest in the information at issue. He noted that there was no evidence before him as to the terms of the contract between Rogers and the accused regarding the confidentiality of the subscriber information. Absent this evidence, he concluded that the information at issue in this case "would tend to disclose intimate details of lifestyle and choices."[117] Because of the nature of the information, the acquisition of such information by law enforcement officials "should be scrutinized by a neutral body, a judicial authority."[118] This did not occur in the case before him. He found that there were no exigent circumstances to justify proceeding without a warrant.

In *R. v. MacInnis*, Ferguson J. criticized earlier cases that had found no reasonable expectation of privacy in cell phone usage data. He considered these cases to be incorrectly decided "because they proceed on the assumption that telephone data is not capable of revealing a biographical core of personal information."[119] As noted earlier, Ferguson J. was of the view that PIPEDA had created a privacy interest in cell phone data in the hands of a private sector company. Beyond this, however, he criticized the earlier cases for being "based on an erroneous characterization of the facts of Canadian lifestyles."[120] In his view, cell phone information is highly sensitive. Even though actual conversations are not part of the data, the data can reveal who called, when and from where. This information "may well reveal the intimate details of the lifestyle and personal choices of the user."[121] The privacy interest would extend to all members of a household using the same service.

The majority of courts, therefore, unlike Justice Leitch in *Wilson*, seem to accept that data cannot be viewed as atomized pieces, but its sensitivity must be evaluated in the context in which it is sought, and the use to which it will be put.[122] Pomerance warns of the risks to privacy posed by viewing information as small fragments in an age of data mining. She writes, "[z]ero plus zero does not always equal zero and, like a jigsaw puzzle, a very clear picture can emerge when otherwise unintelligible pieces are fit together. This process can strike very poignantly at what we call the biographical core."[123] Kerr and McGill refer to the "jigsaw nature of the data/information/knowledge/wisdom chain."[124] They also challenge the approach that views information as "*smaller and smaller bits of data* which, through the reductive process, eventually no longer reveal a biographical core of information."[125] Where identifying information can be linked to information about a per-

117 *Ibid.* at para. 35.

118 *Ibid.*

119 *Ibid.* at para. 49.

120 *Ibid.*

121 *Ibid.* at para. 50.

122 Note that privacy theorist Nissenbaum, *supra* note 98 at 216, has described as an erroneous assumption the view that an "aggregation of information does not violate privacy if its parts, taken individually, do not."

123 Pomerance, *supra* note 48 at 234-235.

124 Kerr & McGill, *supra* note 54 at 431.

125 *Ibid.* at 414. Emphasis in original.

son's activities, then the composite information is information regarding which a person has a reasonable expectation of privacy.

III. OTHER DATA PROTECTION STATUTES

A comparison with the language used in other private sector data protection statutes such as those in Alberta and B.C. might bolster the argument that lawful authority means something less than a warrant, leaving organizations with a fairly broad discretion to disclose. Alberta's PIPA,[126] and B.C's PIPA,[127] both permit disclosure without knowledge or consent for law enforcement purposes, and neither mentions "lawful authority."[128] A similarly worded provision in Saskatchewan's public sector data protection legislation[129] was considered by the Saskatchewan Provincial Court in *R. v. Trapp.*[130] In that case, the public sector statute applied because the internet service provider was a provincially-owned crown corporation. The court found, as a result of the wording of the statute, which placed no limits on the licence granted to private sector companies to disclose information to law enforcement officials, it could not find that the constitutional rights of the accused had been violated.[131]

The provisions in PIPEDA's provincial counterparts are, like s. 7(3)(c.1), permissive and not mandatory. Private sector organizations are required to comply with data protection norms. A private sector organization should be governed by the terms of its privacy policy, which will typically form part of the agreement between it and its customers. In this way, data protection legislation, by requiring private sector organizations to be clear about how they will treat their clients' personal information, may create a reasonable expectation of privacy in that information even in jurisdictions with broad permissive disclosure provisions. A company that says that it will not volunteer personal information to police authorities without its clients' consent is within its rights to insist upon judicial authorization prior to any disclosure.

---

126 *PIPA* (Alberta), *supra* note 25, s. 20(f).

127 *PIPA* (B.C.), *supra* note 25, s. 18(j).

128 A similar kind of provision was considered by the Saskatchewan Provincial Court in *R. v. Trapp*, *supra* note 69. The court found that, as a result of the wording of the statute, it could not find that the constitutional rights of the accused had been violated.

129 *Freedom of Information and Protection of Privacy Act*, 1990-91, c. F-22.01 [FOIPP].

130 *Supra* note 69.

131 Section 29(2) of FOIPP, *supra* note 129, provides: (2) Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed:

. . . .

(g) to a prescribed law enforcement agency or a prescribed investigative body:

(i) on the request of the law enforcement agency or investigative body;

(ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and

(iii) if any prescribed requirements are met

(a) The Investigative Powers for the 21st Century Act and the Technical Assistance for Law Enforcement in the 21st Century Act

In the spring of 2009, the federal government introduced two new Bills, both of which are aimed at updating the criminal law, including powers of investigation, to address issues raised by new technologies. The Bills are intended to implement Canada's obligations under the *Convention on Cybercrime*.[132] The Bills do not represent Canada's first attempt to ratify this Convention. An earlier attempt, the *Modernization of Investigative Techniques Act* (Bill C-74)[133] died on the order paper during the term of the Liberal minority government in 2006. Bill C-74 proved controversial, and it was widely criticized by privacy advocates and ordinary citizens.[134]

The *Investigative Powers for the 21st Century Act* (Bill C-46)[135] and the *Technical Assistance for Law Enforcement in the 21st Century Act* (Bill C-47)[136] each contain provisions that are relevant to the issue of location information in the hands of third parties. For example, in Bill C-46, new provisions for obtaining either production orders or warrants for tracking data set the terms and conditions under which such orders will be granted. The Bill distinguishes between obtaining authorization to track transactions and things, and authorization to track individuals. The tracking of transactions and things requires only a "reasonable suspicion",[137] whereas the tracking of individuals requires the judge to be satisfied that there are reasonable grounds to believe that an offence has or will be committed, and that the tracking of the individual will be of assistance in the investigation.[138] The Bill also provides for judicial authorization to obtain tracking data in the hands of third parties on a reasonable suspicion standard.[139] Thus, even if data tracks the movement of *individuals*, if it is in the hands of a third party, only a reasonable suspicion standard applies to a request for a production order for the data. With the growing involvement of the private sector in collecting location data for a broad range of products and services, the lower threshold is problematic.

It is also significant that Bill C-46 does not affect decisions by third parties in possession of such data to volunteer the information to the police. Section 487.0195 provides:

> 487.0195(1) For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by

---

132 Council of Europe *Convention on Cybercrime*, 23 November 2001, ETS No. 185. The Convention was signed by Canada on 23 November 2001.

133 Bill C-74, *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2004.

134 Daphne Gilbert, Ian R. Kerr & Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" (2007) 51 Crim. L.Q. 469.

135 Bill C-46, *supra*, note 13.

136 Bill C-47, *supra*, note 13.

137 Bill C-46, *supra* note 13, s. 492.1(1).

138 *Ibid.*, s. 492.1(2).

139 *Ibid.*, s. 487.017.

> law from preserving or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.

This does more than leave s. 7(3)(c.1) undisturbed; it goes some way to supporting the view that no warrant or judicial authorization is necessary for the disclosure to law enforcement of information in the hands of third parties.

Bill C-47 would, if enacted, have an impact on some of the issues raised by the case law on access to data in the hands of third party ISPs. In particular, the Bill provides:

> 16. (1) Every telecommunications service provider shall provide a person designated under subsection (3), on his or her written request, with any information in the service provider's possession or control respecting the name, address, telephone number and electronic mail address of any subscriber to any of the service provider's telecommunications services and the Internet protocol address, mobile identification number, electronic serial number, local service provider identifier, international mobile equipment identity number, international mobile subscriber identity number and subscriber identity module card number that are associated with the subscriber's service and equipment.

Such a provision would remove the need for investigators to obtain warrants to access a broad range of subscriber information that would link individuals to activities on the internet, as well as to activities trackable through the use of cell phones or other location-based applications that use telecommunications facilities. Gilbert *et al.* argue that this approach to subscriber data flows from a view that there is a low expectation of privacy in this data.[140] Yet, where the disclosure of this data may have the consequence of revealing one's activities, thoughts and assumptions, it is difficult to see why this lower level of protection is warranted.

These provisions are defended by government as being necessary to ensure that law enforcement and national security officials have quick access to basic information needed to follow leads in developing investigations. They cite uneven practices as necessitating a clear legislative provision:

> [T]he practices of releasing this information to police forces and CSIS vary across the country: some service providers release this information to law enforcement immediately upon request; others provide it at their convenience, often following considerable delays; while others insist on law enforcement obtaining search warrants before the information is disclosed. This lack of national consistency and clarity can delay or block investigations.[141]

---

140 Gilbert *et al.*, *supra* note 134 at 484.

141 Public Safety Canada, "Technical Assistance for Law Enforcement in the Twentieth Century Act" (18 June 2009), online: Public Safety Canada <http://www.publicsafety.gc.ca/media/nr/2009/nr20090618-1-eng.aspx>.

Safeguards to protect privacy are offered in terms of a limited list of persons designated to make the requests under the legislation, and internal as well as external oversight of the exercise of the powers.[142]

In the consultations by Public Safety Canada and Industry Canada related to customer name and address information in 2007, the Office of the Privacy Commissioner of Canada criticized a similar proposal for enhanced access by law enforcement to subscriber information. The Commissioner argued that the proposal lacked the evidentiary basis necessary to justify such changes to the status quo. She argued that s. 7(3)(c.1) of PIPEDA already governed the issue of access by law enforcement to data in the hands of third parties. She stated that she supported certain clarifications to the wording of this section that would reduce some of the uncertainties surrounding its use — particularly the addition of a definition of "lawful authority." She was of the view that with these changes, s. 7(3)(c.1) and PIPEDA as a whole, would suffice to govern access by law enforcement to data in the hands of third parties.[143] The Commissioner also criticized the assumption made in the consultation document (and present as well in Bill C-47) that customer name and address information carried with it a low expectation of privacy. She noted that not all CNA data was publicly available. Further, she observed:

> While some of this information might be considered less sensitive we need to recognize that it is typically not being sought as an end in itself. CNA information may be valuable to LE/NS [law enforcement/national security] agencies specifically because it can provide access to even more sensitive information.[144]

Certainly in the context of internet based activities, CNA information is the key that links a range of internet based activities to a specific individual.

Although s. 16 of Bill C-47 applies only to telecommunications service providers, the impact of this provision on the issues discussed in this paper would be significant. This is particularly the case because so many location-based applications already operate over the mobile networks of telecommunications companies. These are not just applications related strictly to the use of these facilities as a medium for communication; increasingly they relate to global positioning systems, or other applications that run in the background as people carry out day-to-day activities.

Even if enacted, underlying constitutional issues may still affect s. 16 if, for example, it is found to conflict with the *Charter* right to be free from unreasonable

---

142 Only designated persons may make requests for subscriber information (s. 16(3)), and the number of such persons is limited — Bill C-47, *supra* note 13, s. 16(4). Nevertheless, an officer may make a demand without being a designated person in "exceptional circumstances" (s. 17). Records must be kept of all requests (s. 18), and regular internal audits of these records are mandated (s. 20).

143 Jennifer Stoddart, Privacy Commissioner of Canada, "Customer Name and Address (CAN) Information Consultation Document: Response of the Office of the Privacy Commissioner of Canada to Public Safety Canada" (October 2007), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/information/pub/lar_071108_e.pdf>.

144 *Ibid.* at 6.

search or seizure in particular contexts. Bill C-47 also does not resolve the broader issue of law enforcement access to all the different types of location data in the hands of private sector companies. For businesses other than telecommunications companies that collect location data and other customer personal information, the issues around access by law enforcement to this information under permissive data protection legislation remains.

CONCLUSION

Although our activities in public space were once subject mainly to casual observation by others who shared that space, the situation is different in our highly technological and data-driven society. As individuals carry out their daily activities, they leave detailed data trails not just on the internet, but as they move through public space. The old adage that there is no privacy in public spaces is no longer adequate to deal with the nature and amount of data that is gathered about us as we carry out our daily activities. Activities in public space are increasingly represented and recorded as "data." Expectations of privacy in our activities must, therefore, be considered under an information privacy analysis.

In this context, the data protection dimensions of the reasonable expectation of privacy are enormously important. The reduction of our daily activity to a data record — or a series of data records necessitates a change in how we conceive of privacy. Although it is still possible for law enforcement officials to carry out tracking and surveillance activities in their own right, they are increasingly reliant upon data collected and compiled by third parties. As the quality and the detail of that data increases, this creates a highly specific record of individual activities and movements. Indeed, vast quantities of location information are collected by private sector companies — from details of our virtual travels across the internet, to tracking information in the form of cell phone records, transaction data, or data from RFID tags in automated toll passes, swipe cards and other RFID enabled devices.

Data protection legislation inherently creates an expectation of privacy in the data collected by others in private sector contexts. While data protection legislation also creates exceptions to the consent rule for disclosure of this information, the existence of a reasonable expectation of privacy should mean that the exceptions are narrowly construed, and that "lawful authority" must mean express statutory authority or judicial authorization. Any other approach would mean that the private sector collection, use and disclosure of its huge volumes of data would provide a rich resource for law enforcement officials, and an opportunity to do an end run around established privacy norms.

In a similar vein, even absent express "lawful authority" language, the permissive disclosure provisions of statutes like British Columbia and Alberta's *Personal Information Protection Act*s should not be taken to automatically eliminate any reasonable expectation of privacy in the data. Compiled location data, revealing as it does a pattern of movements and associations is highly sensitive information of a kind that it may simply not be reasonable for a third party company to disclose without the request for judicial authorization to establish that the data is being sought for constitutionally legitimate ends.