Privacy and Publicly Available Personal Information

Teresa Scassa[*]

INTRODUCTION

The *Personal Information Protection and Electronic Documents Act* (PIPEDA)[1] creates a consent-based regime for the collection, use and disclosure of personal information. It also creates a number of exceptions to the general requirement of consent. One of these is for publicly available information. This term is given a specific and limited definition in the *Regulations Specifying Publicly Available Information*.[2] Although the categories of publicly available information set out in the *Regulations* have been strictly limited, a recent Alberta Court of Appeal decision that is on appeal to the Supreme Court of Canada[3] has generated discussion about whether information in public view should be added to the list of information that qualifies as "publicly available information." If this question can be posed about information in real space, it can also be asked about information posted online.

The rationale for the exception for publicly available information lies in the fact that such information is of a kind or quality such that either the individual's consent to make it public can be presumed, or its publication is mandated by law in order to serve specific public purposes. Collection, use and disclosure of this information in a manner consistent with these purposes requires no further consent. The core issue to be considered in this article is whether PIPEDA's *Regulations* should be amended to include information in public view. Although the focus is on PIPEDA, reference will also be made to equivalent provisions in the private sector data protection statutes of Alberta[4] and British Columbia,[5] both of which have been

---

[*] Canada Research Chair in Information Law and Professor, University of Ottawa, Faculty of Law, Common Law Section. This paper is based on a report commissioned by the Office of the Privacy Commissioner of Canada (OPC). The views expressed in this article are those of the author and do not necessarily represent the views of the OPC.

1 SC 2000, c 5. PIPEDA governs the collection, use and disclosure of personal information by private sector actors. It applies to federal works, undertakings and businesses across Canada, and to organizations that carry out their commercial activities interprovincially or internationally. It also applies to intra-provincial commercial activities in any province that has not enacted substantially similar legislation.

2 *Regulations Specifying Publicly Available Information*, SOR/2001-7 [*Regulations*].

3 *UFCW-Can, Local 401 v. Alberta (Information and Privacy Commissioner)*, 2012 ABCA 130 (Alta. C.A.); additional reasons 2012 CarswellAlta 1393 (Alta. C.A.); leave to appeal allowed 2012 CarswellAlta 1769 (S.C.C.).

4 *Personal Information Protection Act*, SA. 2003, c P-6.5 [PIPA (Alberta)].

5 *Personal Information Protection Act*, SBC 2003, c 63 [PIPA (BC)].

declared substantially similar to PIPEDA.[6] It is Alberta's exception for publicly available information that will be considered by the Supreme Court of Canada in 2013.

This article begins with a review of the structure of PIPEDA in order to situate the exception within its statutory context. This is followed by a detailed consideration of the exception for publicly available information. The article then offers a discussion of whether the scope of this exception should be expanded, and offers an alternative.

I. THE STRUCTURE OF PIPEDA

Broadly speaking, section 4 of PIPEDA provides that it applies to "organizations,"[7] and to the "personal information"[8] that they collect, use or disclose in the course of "commercial activities."[9] Each of the terms in quotation marks is separately defined in the legislation. Each is also expansively defined, giving PIPEDA a broad application to private sector actors in their collection, use and disclosure of personal information. PIPEDA also applies to the personal information that "is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."[10]

In spite of its broad scope, certain activities are excluded from the application of PIPEDA. For example, to avoid conflict with the *Privacy Act*,[11] the application of PIPEDA to the federal public sector is expressly excluded.[12] PIPEDA also does not apply to "any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect,

---

6 Quebec's *An Act respecting the protection of personal information in the private sector* (QC), RSQ c. P-39.1 [PPIPS], was deemed substantially similar in: *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374, 19 November, 2003. Note that this statute predates PIPEDA. PIPA (Alberta), *supra* note 4, was declared substantially similar by: *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219, 12 October 2004. PIPA (BC), *supra* note 5, was declared substantially similar by: *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220, 12 October 2004. Ontario's *Personal Health Information Protection Act*, SO 2004, c 3, Sch A has also been found to be substantially similar to PIPEDA, but it is applicable only to personal health information in Ontario.

7 An organization is defined as: "an association, a partnership, a person and a trade union." (PIPEDA, *supra* note 1, s. 2).

8 "Personal information" is defined as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." PIPEDA, *ibid.*

9 PIPEDA, *ibid.*, s. 4(1)(a). "Commercial activity" is defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." PIPEDA, *ibid.*

10 PIPEDA, *ibid.*, s. 4(1)(b).

11 RSC 1985, c. P-21.

12 PIPEDA, *ibid.*, s. 4(2)(a).

use or disclose for any other purpose."[13] In a sense, this exclusion merely reinforces that PIPEDA only applies to the collection, use or disclosure of personal information in the course of commercial activities. Purely personal or domestic activities fall outside its scope. The application of the *Act* is also expressly excluded in the case of "any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose."[14] This exception is no doubt intended to balance the privacy rights of individuals in their personal information with freedom of expression values.[15]

Apart from these exceptions, the normative provisions of PIPEDA receive broad application to the collection, use or disclosure of personal information by private sector actors in the course of commercial activities. The core normative provisions of PIPEDA are found in Schedule I, which reproduces the CSA Model Code for the Protection of Personal Information on which the data protection norms in PIPEDA are based.[16] Sections 5 through 10 of PIPEDA either supplement or modify the norms set out in Schedule I.

The cornerstone principle of PIPEDA is consent. Consent is addressed in principle 4.3 of Schedule I, as well as in section 7 of the Act. Principle 4.3 of Schedule I of PIPEDA provides that "[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate." Individuals must be informed of the purposes for which their information will be used or disclosed.[17] The form of consent provided may vary according to the circumstances and the type of information. Generally, the more sensitive information is considered to be, the more stringent will be the consent requirements.[18]

Section 7 of PIPEDA contains a series of exceptions to the requirement of consent. Subsection 7(1) creates exceptions to the consent requirement for the collection of personal information; subsection 7(2) creates exceptions for consent to use, and subsection 7(3) creates exceptions to the requirement of consent for disclo-

---

13 PIPEDA, *ibid.*, s. 4(2)(b).

14 PIPEDA, *ibid.*, s. 4(2)(c).

15 See Teresa Scassa, "Journalistic Purposes and Private Sector Data Protection Legislation: Blogs, Tweets, and Information Maps" (2010) 35 Queen's Law J 733. This article criticizes the way in which this exception is formulated. By excluding the application of PIPEDA, *supra* note 1, from information collected, used or disclosed for the stated purposes, all possible oversight of the way in which this personal information is dealt with (including the reasonableness of the purposes) is precluded. Note that the journalism exception is also at issue in *United Foods*, *supra* note 3.

16 In fact, Schedule I of PIPEDA, *supra* note 1, reproduces, in its entirety, the CSA Model Code. For a discussion of how the CSA Code came to be incorporated within PIPEDA, see: Stephanie Perrin, Heather H Black, David H Flaherty & T Murray Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, (Irwin Law, 2001), pp 13–15.

17 PIPEDA, *supra* note 1, Schedule I, Clause 4.3.2.

18 PIPEDA, *ibid.*, Schedule I, Clause 4.3.6. See, e.g., *Randall v. Nubodys Fitness Centres*, 2010 FC 681 (F.C.), at paras. 41–43; *Englander v. Telus Communications Inc.*, 2004 FCA 387 (F.C.A.), at para. 60 [*Englander*].

sure of personal information. In each of these subsections, there is an exception to the requirement of consent where the personal information is "publicly available information" within the meaning of the regulations. This is not an exception to the *application* of PIPEDA; it is merely an exception to the requirement of consent. The other normative provisions of PIPEDA — such as, for example, the obligation to safeguard personal information — will still apply to publicly available information that is collected, used or disclosed in the course of commercial activity.

(a) The Definition of Personal Information

Data protection legislation in Canada, whether in the private or public sectors, tends to share a common core definition of "personal information." While different statutes vary in terms of whether they enumerate the types of information included within the primary definition, most data protection statutes define personal information as "information about an identifiable individual."[19] This shared definition of "personal information" is important. It has led to the development of a general approach across Canada which is relatively consistent. Given the array of data protection statutes across public and private sectors, and across federal and provincial jurisdictions, and the challenges this poses for compliance, it is helpful to have some common consensus around key terms and principles.

Under PIPEDA, the definition of personal information is not limited to information recorded or stored in any particular format or medium. "Personal information" has been found to include medical or biological data,[20] biometric data,[21] the sound of one's voice,[22] photographic or video images,[23] data,[24] or other written information. The crucial point is that the information must be about an identifiable individual. The individual need not be directly identified by the information; it is enough if the individual can be identified by matching the information with information available from other sources.[25] Thus, for example, other data about the In-

---

19 PIPEDA, *supra* note 1, s. 2. The *Privacy Act*, *supra* note 11, s. 3, defines "personal information" as "information about an identifiable individual that is recorded in any form," and then provides a list of types of information that are included within the definition. Both PIPA (BC), *supra* note 5, s. 1, and PIPA (Alberta), *supra* note 4, s. 1, have definitions of "personal information" that are similar to that in PIPEDA. The comparable Quebec legislation, *supra* note 6, uses slightly different wording, and provides, in s. 2, that "Personal information is any information which relates to a natural person and allows that person to be identified."

20 *Rousseau v. Wyndowe*, 2006 FC 1312 (F.C.); varied on different grounds in 2008 FCA 39 (F.C.A.).

21 *Yeager v. Canada (Minister of Citizenship and Immigration)*, 2008 FC 113 (F.C.). See also *Privacy Act*, *supra* note 11, s. 3.

22 *Wansink v. Telus Communications Inc*, 2007 FCA 21.

23 *Eastmond v. Canadian Pacific Railway*, 2004 FC 852.

24 *Gordon v. Canada (Minister of Health)*, 2008 FC 258.

25 *Gordon, ibid.* See also: Teresa Scassa, "Geographic Information as Personal Information", (2010) 10:2 Oxford University Commonwealth Law Journal 185.

ternet-based activities of individuals — including that collected by cookies — is personal information if it can be linked to an identifiable individual.[26]

The definition of "personal information" in PIPEDA has been described as "very far reaching."[27] Indeed, given the structure and objectives of data protection statutes, it has not made sense to limit the definition of personal information.[28] Specific limitations required in particular contexts are introduced in the form of limits on the application of the legislation or as exceptions to requirements for consent to collection, use or disclosure, as is the case with publicly available information.

(b) Personal Information v. Private Information

"Personal information" is not synonymous with "private information." Thus publicly available information is not disqualified from being personal information simply by virtue of the fact that it is public.[29] Controversially, in *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*,[30] the majority of the Alberta Court of Appeal ruled that a driver's licence plate number was not personal information. In reaching that decision, they stated: "It is also contrary to common sense to hold that a vehicle licence number is in any respect private."[31] Yet whether the number is on display or not is clearly irrelevant to the issue of whether the number is personal information. Indeed, if public information were automatically disqualified from being personal information, there would be no need for the statutory exception for publicly available information. In its subsequent decision in *United Food and Commercial Workers, Local 401 v. Alberta (Attorney General)*,[32] the Alberta Court of Appeal noted that under the province's *Personal Information*

---

26 PIPEDA Case Summary #2003-162, "Customer complains about airline's use of "cookies" on its Web site", <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030416_7_e.cfm>. See also: Office of the Privacy Commissioner of Canada, *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing*, May 2011, <http://www.priv.gc.ca/resource/consultations/report_201105_e.pdf>, at 24 [*Online Tracking*].

27 *Johnson v. Bell Canada*, [2008] F.C.J. No. 1368, 2008 FC 1086 at para. 30. For a detailed discussion of the meaning of "personal information", see Scassa, *supra* note 25.

28 Lisa M. Austin, "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices", (2006-2007) 44 Can. Bus LJ 21 at 52, also argues for a broad interpretation of "personal information".

29 See, e.g.: *Re Synergen Housing Co-op Ltd.*, Order No. P2010-003, Alberta OIPC, <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2636>.

30 *Leon's Furniture Ltd. v. Alberta (Information & Privacy Commissioner)*, 2011 ABCA 94; leave to appeal refused 2011 CarswellAlta 1938 (S.C.C.) [*Leon's Furniture*].

31 *Ibid.* at para. 50. Conrad J, in her dissenting opinion, at paras. 112-113, makes this distinction between the private sphere protected by the reasonable expectation of privacy, and the broader goals of data protection legislation.

32 *Supra* note 3.

Protection Act (PIPA(Alberta)),[33] "'personal' information is not the same as 'private' information."[34]

The distinction between personal information and private information is linked to the purpose of data protection legislation, which, in the case of PIPEDA, is set out in section 3:

> 3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

The statute is aimed at providing a regime to govern the manner in which organizations collect, use or disclose the personal information of individuals in the course of commercial activity, in a manner that is respectful of the privacy rights of individuals. This applies to all information. PIPEDA gives individuals a measure of control, through the central concept of consent, over their personal information. The statute has numerous provisions which override the principle of consent in specific circumstances, where other interests, both public and private, outweigh the right of the individual to control uses of their information.[35]

By contrast, a right to privacy, such as that protected by section 8 of the *Charter*,[36] defines certain spheres related to the individual (their person, their home, and their "core biographical information")[37] into which the state may not intrude, unless that intrusion can be justified as a reasonable limit on the privacy right that is demonstrably justified in a free and democratic society.[38] Statutory torts of invasion of privacy offer individuals recourse against anyone (whether a state actor or a private actor) who intentionally invades their privacy. In both the *Charter* and the tort contexts, the issue is whether the individual's sphere of privacy is invaded, and in both contexts the analysis may include a consideration of whether the individual had a reasonable expectation of privacy in the circumstances.[39] Whether informa-

---

33 *Supra* note 4.

34 *United Food*, *supra* note 3 at para. 10.

35 Exceptions to the rule of consent to collection of information are found in s. 7(1) of PIPEDA, *supra* note 1. Exceptions to consent for use are found in s. 7(2), and exceptions to consent for disclosure are in s. 7(3).

36 Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11, s. 8 [*Charter*].

37 This framework is described and discussed, for example, in: *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at paras. 19–24.

38 *Charter*, *supra* note 36, s. 1.

39 In the *Charter* context, see, for example, the discussion of the reasonable expectation of privacy in *R. v. Tessling*, *supra* note 37, at paras. 19–24. The principle is also evident in tort cases. See the discussion in: Elizabeth Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places", (2000) 50 U of T LJ 305, and Teresa Scassa, "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy", (2009) 7:2 CJLT 193.

tion or activities are made public or kept private is therefore often relevant in these contexts. For example, Canadian courts dealing with tort claims and in criminal cases have held that there is little or no expectation of privacy in activities that take place in public,[40] although other courts have added some nuance to this view.[41]

This notion of "reasonable expectation of privacy" is relevant in tort and *Charter* contexts because there is no violation of privacy rights if the individual had no reasonable expectation that their activities would be private. In *United Food*, the Alberta Court of Appeal was critical of the fact that the private sector data protection legislation did not create a broad exception for information "that is personal, but not at all private."[42] Without citing any examples, the Court stated that "the comparative statutes in some provinces exempt activity that occurs in some public places."[43] Yet the only other provinces with private sector data protection statutes are BC and Quebec, and neither statute contains such an exception. The court is most likely referring to the statutes which, in some provinces, create torts of invasion of privacy, and which set certain contextual boundaries for the torts.[44] This type of legislation is not at all equivalent. It may be appropriate that an individual's ability to allege a tortious invasion of their privacy be considered in light of circumstances that include whether they were engaged in activity in a public place. However, such considerations are not relevant in the data protection context, where the issue is not whether individuals have an *expectation of privacy* in their personal information; rather, the issue is one of their ability to control how and when their personal information is collected, used or disclosed.[45] Data protection laws essen-

---

40 See, for example, *Druken v. R.G. Fewer & Associates Inc.*, [1998] N.J. No. 312, 1998 CarswellNfld 289 (T.D.), at para. 43. 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), 88 C.C.C. (3d) vi (note) (S.C.C.); *R. v. Hounsell*, [1994] N.J. No. 319, 1994 CarswellNfld 343 (Prov. Ct.); *R. v. Abbey*, 2006 CarswellOnt 7381, [2006] O.J. No. 4689 (S.C.J.).

41 For example, in *Tremblay c. Compagnie d'assurances Standard Life* the Quebec Court of Appeal affirmed the trial judge's finding that while in general there might be no reasonable expectation of privacy in activities carried out in public, the nature and duration of surveillance activities may be such that an individual's privacy rights are violated because of the cumulative effect of monitoring of daily activities. At trial, Soldevila J. observed : « 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. » *Tremblay c. Cie d'assurances Standard Life*, [2008] J.Q. No. 5252, 2008 QCCS 2488 at para 59, ; affirmed 2010 CarswellQue 4440 (C.A.); varied 2010 QCCA 933 at para. 96.

42 *United Food*, *supra* note 3 at para. 77.

43 *Ibid.* at para. 73.

44 See, for example, *Privacy Act*, RSBC 1996, c. 373 (British Columbia); *The Privacy Act*, RSM 1987, c. P125 (Manitoba); *The Privacy Act*, RSS 1978, c. P-24 (Saskatchewan); *Privacy Act*, RSN 1990, c. P-22 (Newfoundland and Labrador); *Civil Code of Québec*, SQ 1991, c. 64, arts 35–41.

45 See, e.g., the dissenting opinion of Conrad J. in *Leon's Furniture*, *supra* note 30 at paras. 111-112.

tially set a code of conduct for organizations engaged in commercial activities, and they set boundaries as to how personal information may be exploited in these contexts. In such circumstances, whether the information is "public" or "private" is irrelevant to whether information is personal information governed by the data protection statute.[46] There is no obvious reason why an exception to the law should be created so as to permit companies to cull personal information about individuals from multiple sources regarding their movements in public spaces without their consent. It is important to note that video surveillance cameras and cell phone location information could both constitute this kind of information.

II. PUBLICLY AVAILABLE INFORMATION

Certain categories of information known as "publicly available information" are the subject of exceptions to the rules of consent under section 7 of PIPEDA.[47] These categories are identified in the *Regulations Specifying Publicly Available Information*.[48] The way in which these exceptions are structured means that "publicly available information" may still be considered personal information.[49] However, consent is not required for its collection, use or disclosure in certain prescribed circumstances. The application of the other data protection norms is not precluded by the fact that personal information is also publicly available information. Thus an organization that collects, uses and discloses publicly available information would still be required to comply with the norms regarding access, or the safeguarding of personal information. In Case Summary #2009-004,[50] for example, the Assistant Privacy Commissioner recommended that the respondent organization modify its website to specify that it collects publicly available information in order to satisfy the openness requirement of PIPEDA.

---

46 It may, however, be relevant to determining the degree of sensitivity of the information. See, e.g., *Re K.E. Gostlin Enterprises*, Order P05-01, OIPC BC, <http://www.oipc.bc.ca/PIPAOrders/2005/OrderP05-01.pdf> at para. 58. The conflation of "reasonable expectation of privacy" principles with private sector data protection legislation is evident in the decision at first instance in *UFCW-Can, Local 401 v. Alberta (Information and Privacy Commissioner)*, 2011 ABQB 415; varied 2012 CarswellAlta 760 (C.A.); additional reasons 2012 CarswellAlta 1393 (C.A.); leave to appeal allowed 2012 CarswellAlta 1769 (S.C.C.). There, the judge found that "[t]here is no rational connection between protecting privacy when the individuals in question are in public view. There is no right to 'practical anonymity'" (at para. 155). The failure to find a rational connection between regulating the capturing of information in public view and data protection is a failure to understand the goals and structure of the legislation.

47 These are found in PIPEDA, *supra* note 1, at paras. 7(1)(d), 7(2)(c.1), and 7(3)(h.1).

48 *Regulations*, *supra* note 2.

49 For example, in PIPEDA Case Summary #2009-004, No Consent Required for Using Publicly Available Personal Information Matched with Geographically Specific Demographic Statistics, [2009] CPCSF No. 4, <http://www.priv.gc.ca/cf-dc/2009/2009_004_0109_e.cfm>, the Assistant Privacy Commissioner refers to "publicly available personal information" in contrast to "personal information subject to consent requirements."

50 PIPEDA Case Summary #2009-004, *ibid.*

Publicly available information also remains subject to section 5(3) of PIPEDA which provides that "[a]n organization may collect, use or disclose personal information *only for purposes that a reasonable person would consider are appropriate in the circumstances*."[51] In Case Summary #2009-015, the Assistant Privacy Commissioner stated that section 5(3) applied to the exceptions to consent in section 7 of PIPEDA, including those relating to publicly available information.[52] This means that any collection, use or disclosure of publicly available information is only exempted from the consent requirements where the collection, use or disclosure is for a purpose that a reasonable person would consider appropriate in the circumstances.

The categories of "publicly available information" are created to address personal information that is made publicly available in certain contexts and for certain purposes.[53] PIPEDA and the equivalent statutes in Alberta and BC recognize that where certain information has been made publicly available, it would not make sense to require additional consent to permit its collection, use or disclosure for those purposes. In other words, "this information should continue to be accessible to an organization for its primary purpose without the need to obtain the individual's consent."[54] However, if the information is used for purposes other than those for which it was made public, "the use of the information for secondary purposes should be subject to the same fair information principles that apply to other types of personal information."[55] It is also important to note that the exception only applies to information gathered from publicly available sources. If the same information is collected from a different source, the information is not considered "publicly available" and there is no exception to the requirement of consent.[56]

To qualify as publicly available, information must be available to the public without limitation or restriction.[57] Information that is only available for a fee is not publicly available information. Each of the categories of publicly available information identified in the regulation shares this feature. In the case of information appearing in magazines and newspapers, there is generally free access through pub-

---

51 PIPEDA, *supra* note 1, s. 5(3). Emphasis added.

52 PIPEDA Case Summary #2009-015, Individual's creditor leaves legal debt-recovery document at his workplace, [2009] CPCSF No 15, at para. 11, <http://www.priv.gc.ca/cf-dc/2009/2009_015_0316_e.cfm>.

53 For example, the PIPA Information Sheet states: "By defining the categories of personal information that is publicly available information, the Act makes it clear that not all personal information in the public domain can be considered publicly available information under PIPA." (Office of the Information and Privacy Commissioner of Alberta, "Publicly Available Information", *Personal Information Protection Act*, Information Sheet 9, September 2006; Revised May 2010, <http://servicealberta.ca/pipa/documents/InfoSheet9.pdf>, at 1 [PIPA Information Sheet].

54 PIPA Information Sheet, *ibid.* at 1.

55 *Ibid.*

56 *Ibid.* at 2. See also *Citi Cards Canada Inc. v. Pleasance*, 2010 ONSC 1124, [2010] O.J. No. 1175, at para. 26, ; affirmed 2011 ONCA 3, [2011] O.J. No. 15.

57 PIPA Information Sheet, *supra* note 53 at 2.

lic libraries. Information will also still be considered to be publicly available even where it is only accessible from one location. An example might be a public registry that must be consulted at a particular government office. The main condition is that information must be openly available to the public for consultation. By contrast, information that is available only to those who subscribe to a service or who meet eligibility requirements is not publicly available information.

(a) Publicly Available Information in Substantially Similar Legislation

As noted above, both PIPA (Alberta) and PIPA (BC) share a similar approach to PIPEDA with respect to publicly available information. Each of these statutes creates an exception to the requirement of consent for the collection, use or disclosure of personal information where it is available to the public from a source that is recognized in regulations enacted pursuant to the statute. In each of these provincial statutes, the regulations establish a closed list of categories of publicly available information[58] that are essentially the same as those in PIPEDA's *Regulations Specifying Publicly Available Information*. In Alberta, the equivalent regulations have come under challenge in *United Food*, where the Alberta Court of Appeal objected to what it called the "artificially narrow" definition of publicly available information.[59]

In Quebec, section 1 of the *Act respecting the Protection of Personal Information in the Private Sector* provides that it does not apply to "information which by law is public."[60] This must be understood with reference to section 57 of the *Act respecting Access to documents held by public bodies and the protection of personal information*[61] which sets out that information which can be considered by law to be public. This information consists of categories of information in the hands of public bodies. While PIPEDA and the PIPA statutes of Alberta and BC include certain government information (such as registry information and court and tribunal information) in the definition of "publicly available information," their categories of "publicly available information" include more than just public sector information. Thus, the Quebec legislation does not exclude from its application information in telephone directories, business or professional directories, or print or electronic publications that are available to the public.

(b) The Definition of Publicly Available Information

An exception to the rules of consent for the collection, use and disclosure of personal information under paragraphs 7(1)(d), (2)(c.1) and (3)(h.1) of PIPEDA is available where the personal information "is publicly available and is specified by

---

58 In Alberta, see: *Personal Information Protection Act Regulation*, Alberta Regulation 366/2003, s. 7. In BC, see *Personal Information Protection Act Regulations*, BC Regulation 473/2003, s. 6.

59 *Supra* note 3 at para. 77.

60 PPIPS, *supra* note 6, s. 1.

61 RSQ chapter A-2.1

the regulations."[62] The *Regulations Specifying Publicly Available Information*[63] create a closed list of five categories of "information and classes of information."[64] Each of these is considered in turn below.

(i) Telephone Directory Information

Paragraph 1(a) of the *Regulations* characterizes as publicly available information:

> (a) personal information consisting of the name, address and telephone number of a subscriber that appears in a telephone directory that is available to the public, where the subscriber can refuse to have the personal information appear in the directory;

In order to qualify as publicly available information, the directory must relate to telephone services, it must be publicly available (and not a private or in-house directory),[65] and subscribers must have the option to decline to have their information included.[66] The regulation is crafted so as to include most standard telephone directories, but not to go beyond this type of directory. In Case Summary #2009-04, the Assistant Privacy Commissioner found that a company that took telephone directory information and filtered it using Statistics Canada anonymized geodemographic information for particular neighbourhoods, did not collect, use or disclose personal information without consent, as the directory information was publicly available, and the correlated geodemographic information was not personal information.[67]

It is interesting to note that in Case Summary #2009-004, although the regulations did not explicitly place a limit on the purposes to which directory information could be put, the Assistant Privacy Commissioner applied the general restriction found in section 5(3) of PIPEDA, which limits the collection, use and disclosure of personal information to purposes which a reasonable person would consider appropriate in the circumstances. The Assistant Privacy Commissioner noted in this case that "in making telephone directory information publicly available, Parliament rec-

---

62 PIPEDA, *supra* note 1, at paras. 7(1)(d), 7(2)(c.1), and 7(3)(h.1).

63 *Regulations*, *supra* note 2.

64 PIPEDA, *supra* note 1, s. 26(1)(a.1).

65 According to the PIPA Information Sheet, information must be "publicly available" to qualify for this exception. "Publicly available" means "that any member of the public must be able to have access to the information. There can be no restrictions on who may have access to the information." Thus information only available to members or subscribers of a service would not qualify. PIPA Information Sheet, *supra* note 53 at 2. The Information Sheet also provides that the availability to the public must be regular, and not *ad hoc* or on a case by case basis.

66 *Englander*, *supra* note 18 at paras. 54-55.

67 Case Summary #2009-004, *supra* note 52 at para. 42. She found that the process used by the direct marketing company "does not change the status of the White Pages information from publicly available personal information to personal information subject to consent requirements." (at para. 42).

ognized that it could and would be used for commercial marketing purposes."[68] Thus it was a use that fell within the parameters of section 5(3).[69]

In *Englander v. Telus*,[70] the Federal Court of Appeal ruled that paragraph 1(a) of the *Regulations Specifying Publicly Available Information* applied where

> . . . personal information consisting of the name, address and telephone number of a subscriber already appears in a publicly available telephone directory. They enable organizations to collect, use or disclose that existing information for their own purposes. But the provisions do not, and indeed cannot, apply to the very organization that initially collects the information for the purpose of publishing a telephone directory that will, once published, become publicly available.[71]

Thus an organization in the business of compiling such a directory (as opposed to using one already available) must still comply with PIPEDA's norms regarding consent.

Both Alberta and BC contain largely similar provisions with respect to telephone directory information.

(ii) Professional or Business Directories

Paragraph 1(b) of the *Regulations* characterizes as publicly available information:

> (b) personal information including the name, title, address and telephone number of an individual that appears in a professional or business directory, listing or notice, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the directory, listing or notice;

The exception for publicly available information in professional or other directories removes the need for consent where the collection, use or disclosure of the personal information "relates directly to the purpose for which the information appears in the directory, listing or notice."[72] While such purposes might be limited to contacting the named individuals for business-related reasons, they could potentially be broader. In Case Summary #2005-297,[73] however, the Assistant Privacy Commissioner found that a university published faculty email addresses on its web site in order to permit faculty members to be contacted for reasons that furthered the university's interests. In consequence, it was not consistent with these purposes for an organization to use this information to market season tickets for a sports team. The

---

68 *Ibid.*

69 The same requirement of collection, use and disclosure for "reasonable purposes" in the case of PIPA (Alberta) is referenced in PIPA Information Sheet, *supra* note 53 at 3.

70 *Englander*, *supra* note 18.

71 *Ibid.* at para. 54.

72 The PIPA Information Sheet, *supra* note 53 at 3 states that "[r]elates directly to" means that the collection, use or disclosure "must have a *reasonable and direct connection* to that purpose." [Emphasis in original.]

73 Case Summary #2005-297, Unsolicited email for marketing purposes, online: <http://www.priv.gc.ca/cf-dc/2005/297_050331_01_e.cfm>.

use therefore fell outside the scope of the exception for publicly available information.

The exception is broad enough to include electronic and online directories.[74] This raises an interesting question about whether a social networking site such as LinkedIn[75] might be considered to be a "professional or business directory" within the meaning of the *Regulations*. If it were to be so considered, then the consent norm would not apply to the collection, use or disclosure of "personal information" for the purpose for which it is included on the site. Not only is the nature and amount of personal information on LinkedIn much more extensive than that in traditional professional or business directories (LinkedIn subscribers often provide a considerable amount and variety of personal information), it might be quite challenging to clearly identify the range of purposes for which individuals have supplied this information (to stay in touch with friends/business contacts, to showcase their achievements, to solicit business, etc.). This would make it extremely difficult to determine the parameters of the exception, as the purposes for which information is made available on the site will vary from individual to individual. In addition, it should be noted that section 5(3) of PIPEDA would limit the purposes for which information is collected, used or disclosed to ones which a reasonable person would consider reasonable in the circumstances. There would be some purposes which would fall outside the reach of this clause — such as, for example, targeted marketing of products unrelated to the individual's business or profession.

It is important to note, however, that the exception in the *Regulations* is for professional or business directory information that is *publicly available*. The contents of LinkedIn are not genuinely publicly available. While small amounts of LinkedIn information are available from a general online search, full details are only available to members of the site. In order to become a member, it is necessary to create an account by providing personal information to the social networking site.

Both PIPA (BC) and PIPA (Alberta) include professional or business directory information in their categories of publicly available information. As is the case with the PIPEDA *Regulations*, Alberta explicitly limits the collection, use and disclosure of this information without consent to the purposes for which it appears in the directory. The BC regulation does not contain this express limitation. However, it provides that such directory information is not eligible for the exception unless "the individual is permitted to refuse to have his or her personal information included in the directory."[76]

---

74 For example, in Case Summary #2005-297, *ibid.*, the Assistant Privacy Commissioner of Canada considered that a university's online faculty directory fell within the scope of the exception for professional or business directories.

75 LinkedIn, online: <http://www.linkedin.com>. Note that LinkedIn claims to have over 120 million professionals as members as of August 4, 2011. See online: <http://press.linkedin.com/about>.

76 BC *Personal Information Protection Act Regulations*, *supra* note 58, s. 6(1)(b).

(iii) Registry Information

Paragraph 1(c) addresses a category of publicly available information that has government as its source. It refers to:

> (c) personal information that appears in a registry collected under a statutory authority and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry;

Thus, for example, the public information in a land titles registry would fall under this exception. Such information could be collected, used and disclosed without consent, so long as its use "relate[s] directly to the purpose for which the information appears in the registry."[77] In one case, the Assistant Privacy Commissioner found that any collection, use or disclosure under this exception must be for a purpose that a reasonable person would consider reasonable in the circumstances, in accordance with section 5(3) of PIPEDA.[78] In the case of information that has been made publicly available under statutory authority, it is likely that there will be some reasonably clearly articulated purpose for which the information is made available, and which can be used to place limits on how the information may be used without the data subject's consent. For example, in Case Summary #2009-020, the Assistant Privacy Commissioner ruled that the purpose of the registry set up under the *Bankruptcy and Insolvency Act*[79] was to further the purpose of that statute, which was, in part, "to establish a way for creditors to establish their claims and be repaid."[80] The use of the information for other purposes would not fall within the exception.[81]

Both PIPA (BC) and PIPA (Alberta) provide for an exception for registry information in their regulations governing publicly available information. In Alberta,

---

77 PIPEDA Case Summary #2009-020, *Publicly available information about individual's bankruptcy cannot be disclosed for debt-collection purposes without her consent*, [2009] C.P.C.S.F. No. 20, online: <http://www.priv.gc.ca/cf-dc/2009/2009_020_1210_e.cfm>.

78 *Ibid.* In Alberta, see *Alberta Motor Association Insurance Company Investigation Report*, P2008-IR-001, online: <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2271>, where the Office of the Information and Privacy Commissioner expressed the view that it was legal to collect information about an individual's bankruptcy from the Personal Property Registry where the purpose for collection was an insurance fraud investigation.

79 RSC 1985, c. B-3.

80 PIPEDA Case Summary #2009-020, *supra* note 77 at para. 11.

81 In this case, the creditor disclosed information about the complainant's bankruptcy to her siblings in an attempt to recover the amount of the debt from them. The Assistant Privacy Commissioner found that this fell outside the purposes for which the registry was established. Note that in PIPEDA Case Summary #2009-021, *Disclosure complaint against bank deemed not well-founded because the information came from public records*, [2009] C.P.C.S.F. No. 21, online: <http://www.priv.gc.ca/cf-dc/2009/2009_021_1223_e.cfm>, the Assistant Privacy Commissioner found that the consent was not required for the collection and use by a debt collection agency of information from a public land registry, because that information was publicly available information. The information consisted of the fact that the complainant was the co-

the limitation on the collection, use or disclosure of this information without consent is only for the purpose for which the information appears in the registry, as is the case under PIPEDA. However, the wording of the Alberta exception requires that purpose to be "an established purpose of the registry,"[82] suggesting that specific purposes must be found in the enabling legislation or in regulations or policy documents relating to the registry.

(iv) Records of Judicial or Quasi-Judicial Bodies

Paragraph 1(d) of the *Regulations* includes within the definition of publicly available information personal information that is found in records or documents of courts or tribunals:

> (d) personal information that appears in a record or document of a judicial or quasi-judicial body, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document;

The documents must be ones that are made available to the public, and the exception only applies where the information is used for a purpose that relates directly to that which lies behind its inclusion in the record or document. In Case Summary #2009-015, the Assistant Privacy Commissioner found that although a statement of claim was a court record, access to such documents was not unlimited, as courts retained discretion over the safeguarding of their own records, and had a right to deny access to them for improper purposes. As such, although court records could be consulted by the public, a plaintiff did not have "the unfettered right to distribute the contents of a court file or pleadings to third parties outside the litigation."[83]

Most court and tribunal decisions are publicly available as part of the open courts principle, and a wide range of other documents related to the legal process are available for consultation at court houses or at the offices of administrative agencies. Increasingly, material of this kind is being made freely available online. The OPC has expressed concerns in the past over the publication of administrative tribunal decisions online, and the privacy implications this may have for individuals. Many of these implications go beyond the contexts addressed by PIPEDA. PIPEDA applies to the collection, use or disclosure of personal information in the

---

owner of the residence that corresponded to the home address on her credit card account. The issue of the purposes of the registry was not specifically discussed.

82 PIPA (Alberta), *supra* note 4, s. 7(c). According to the Office of the Information and Privacy Commissioner of Alberta, such purposes may be express — as set out in the enabling legislation, for example — or implied in any government policy established pursuant to an Act or regulation. (PIPA Information Sheet, *supra* note 53 at 4). Note that the exception also refers to governmental and non-governmental registries. Non-governmental registries may be operated by an organization or a local public body acting under the authority of a provincial Act or regulation. (PIPA Information Sheet, *supra* note 53 at 5).The BC *Regulation* refers to registries "to which the public has a right of access." (*supra* note 58, s. 6(1)(c)), so long as it is collected "under the authority of an enactment, the laws of the government of Canada or a province or the bylaws of a municipality or other similar local authority in Canada."

83 PIPEDA Case Summary #2009-015, *supra* note 52.

course of commercial activities, and some of the privacy concerns that relate to administrative tribunal decisions stem from the potential for nosy neighbours, co-workers, ex-spouses or even malefactors to browse electronic decisions for information about individuals. These activities would not be captured by PIPEDA in any event.

The fact that such information may be found online does not really change the scope of the exception — the information would still be considered "publicly available" if members of the public had to go down to the courthouse to request access to a file. Nevertheless, it does change the scale of activities in relation to such information. It makes the personal information contained in these documents very easily accessible and searchable, and very inexpensive to collect and compile. Nonetheless, as noted above, the exception is fairly limited; to qualify for the exception, the purpose for which the information is collected, used or disclosed must be consistent with the purpose for which the information appears on the record.[84] It must also be a purpose that a reasonable person would consider appropriate in the circumstances, as per section 5(3) of PIPEDA.

The limitation to purposes for which information appears on the record can be difficult to apply in the case of court and tribunal records. Often there are multiple purposes for which information is made public. In the judicial or administrative tribunal context, for example, the information may be included to meet any one or more of the following purposes: to provide an accurate record of proceedings; to satisfy the open courts principle; for deterrent effect; to educate the public about an agency mandate; or to provide transparency and accountability.[85] In this respect, there may be some tension between the purpose for which *specific* information appears on the record and the purpose for which records are kept generally. The Office of the Privacy Commissioner of Canada's Guidance Document on *Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals* notes that many of the objectives of courts and tribunals in publishing their decisions can be achieved without publishing all of the personal information contained in the decisions.[86] Recognizing the difficulty in identifying the purposes for which the personal information is recorded under a similar exception in Alberta's PIPA, the Office of the Alberta Information and Privacy Commissioner advises that "[i]f the purpose cannot be determined from information published by the body or specific statements in the record itself, an organization should determine whether a reasonable person would consider the collection, use or disclosure of personal information appropriate in the circumstances."[87] No such exception is present under PIPA (BC) — court and tribunal records do not constitute "publicly available infor-

---

84 For example, in PIPEDA Case Summary #2009-015, *ibid.*, the Assistant Privacy Commissioner found that the disclosure of a statement of claim had to relate directly "to the purpose of advancing a claim in a court of law."

85 Some of these purposes are addressed in OPC Guidance Document, *Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals*, February 2010, online: <http://www.priv.gc.ca/information/pub/gd_trib_201002_e.cfm> [*Guidance Document*].

86 *Guidance Document*, *ibid.*

87 PIPA Information Sheet, *supra* note 53 at 6.

mation" for the purposes of private sector data protection legislation in that province.

(v) Published information

Paragraph 1(e) of the *Regulations* creates an exception to the consent provisions for:

> (e) personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information.[88]

In order to qualify under this section, the information must be contained in a "publication," whether in print or electronic form. A further limit on the exception is that the individual data subject must be the person who provided the information to the publication. Thus, a report on another person's activities, or an unauthorized biography, could not be considered to fit within the scope of this exception.[89] It is important to note that this exception is in many ways broader than the other exceptions because the scope of the collection, use or disclosure without consent is not limited to the purposes for which the information was provided. Thus, so long as the data subject provided the information to the publication, it may be collected, used or disclosed, presumably for any purpose, subject to section 5(3), without the data subject's consent.

It is an open question whether information posted online by individuals, whether in blogs, tweets or on social networking sites constitutes a "publication" for the purposes of this exception. While the exception refers to publications in "electronic" form, not all digital publications will be likely to be considered publicly available. As noted in the earlier discussion of LinkedIn, most social networking sites are not truly "public." Only members — those who create accounts — are given access to the information on the public pages of the site.

The sheer volume of information that may be posted on social networking sites, on blogs or on personal websites by far exceeds the volume of material available through traditional publishing media. There is generally little or no mediation of the content of what is posted online by individuals, and the vast majority of those who post information will have little or no experience in publishing.[90] They may also be unaware of the legal consequences that might flow from the publication of their material. Further, the goals and objectives of those who post information may vary enormously. While some may wish to communicate with the world

---

88 *Regulations*, *supra* note 2, s. 1.

89 In *Re Brubaker*, Order No P2008-010, [2010] A.I.P.C.D. No. 46, online <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2662>, an adjudicator under Alberta's PIPA found that in a case where information had been gathered about police officers' conduct from multiple newspaper articles and letters to the editor, that each letter or article would need to be reviewed separately in order to determine whether the individual officers referred to in each item could be considered to have provided that information. See also PIPA Information Sheet, *supra* note 53 at 6.

90 Note that the PIPA Information Sheet, *ibid.* at 6, cautions that not all print publications are equally reliable and reputable, and warns organizations not to rely on the publicly available provision "if there is any uncertainty as to the source of the information."

at large, others may chiefly be trying to share photographs within their family circle, or to share information with like-minded individuals. It is by no means clear that the majority of those who post content on the internet consider themselves to be communicating to a broad public rather than to limited or private audiences. A recent report by the Office of the Privacy Commissioner of Canada, suggests that in some cases those who create and post content to social networking sites do so because of peer pressure.[91] This calls into question whether individual posters of information intended to make the information publicly available in a broad sense.

Serious consideration must be given to whether any source that provides completely unmediated information should be considered a source of "publicly available information". PIPEDA and its norms can serve as an important protection for the personal information of individuals. To remove the core of that protection in a context where individuals are relatively vulnerable, and where there are no checks and balances, seems problematic. In all other existing categories of publicly available information such checks and balances exist, and there is typically an entity that can be held accountable for improperly making information publicly available.[92]

Another difficulty with information posted on social networking sites, blogs or other internet fora is that it is not always clear *who* has made the information available.[93] For example, a party may post photographs that contain the personal information of others without the knowledge or consent of those individuals. While this kind of disclosure (for domestic or private purposes) is not caught by PIPEDA, the collection, use and disclosure of the information contained in the photo (video or text document) by an organization in the course of commercial activity without the consent of the data subject(s) would fall outside the scope of the exception in paragraph 1(e) of the *Regulations* in the case of third party information. This is because this exception requires the data subject to be the source of the personal information in the publication.

A further, and serious consideration, is that social networking sites are widely used by minors. A recent study estimates that millions of Facebook users are under the age of 13.[94] In the U.S., where special legislation aims to protect children's online privacy, the FTC has acknowledged that the law is of little use in contexts where children provide inaccurate information about their age in order to obtain

---

91 *Online Tracking*, *supra* note 26 at 17.

92 For example, in *Englander*, *supra* note 18, the telephone company was held responsible for not properly informing customers about their right to have their listing information excluded from the telephone directory.

93 The Decima Research, Research Report: Focus Testing Privacy Issues and Potential Risks of Social Networking Sites, 20 March 2009, <http://www.priv.gc.ca/information/survey/2009/decima_2009_02_e.cfm> [Decima Research] at 7, indicated that not only do many users post photographs to social networking sites that include other individuals, but many also tag these photos so as to identify the individuals in them.

94 Wailin Wong, "Millions of underage kids use Facebook, Consumer Reports says," 10 May 2011, Chicago Tribune <http://www.chicagotribune.com/business/breaking/chibrkbus-millions-of-kids-under-age-13-use-facebook-consumer-reports-says-20110509,0,4123052.story>.

access to otherwise restricted online services.[95] Although Facebook accounts are in theory only available to those over the age of 13, it is well known that this restriction is easy to circumvent. Apart from these vulnerable users under the age of 13, millions more will be between 13 and 18 years of age, and thus still minors. The FTC notes concerns "that teens may not be fully aware of the consequences of what they do,"[96] with the result that "teens may voluntarily disclose more information than they should."[97] These findings are supported by recent Canadian research which found that the high risk behaviour of youth that is found in other contexts may also extend to the internet.[98] A report by the Office of the Privacy Commissioner of Canada also notes that younger children using social networking sites consider that the audience for their posted information is other children.[99] The use by third parties of information posted by teens on Facebook was identified in one U.S. study as one of the main privacy risks of such sites.[100] Any inclusion of social networking site information in the category of "publicly available information" would expose potentially vast quantities of personal information of minors to collection, use or disclosure without consent.

Alberta and BC both include information in a publication as "publicly available information." Both provincial exceptions refer to print or electronic publications and both expressly include, but do not apparently limit, the exception to magazines, books or newspapers. In Alberta, it must be "reasonable to assume that the individual that the information is about provided that information."[101] No such express limitation is found in the BC regulation.[102]

III. DISCUSSION

As noted above, "publicly available information," as defined in the *Regulations Specifying Publicly Available Information*, is exempt from the requirement of consent for its collection, use or disclosure. However, the exception is narrowly framed. It is available only where the information is collected, used or disclosed for

---

95 The legislation in question is the *Children's Online Privacy Protection Act of 1998*, 15 U.S.C. §§6501-6506, P.L. 105-277. See the discussion in Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policy Makers*, Preliminary FTC Staff Report, December 2010, <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> [FTC Framework] at 16.

96 *Ibid.*

97 *Ibid.* at 16.

98 Avner Levin, et al, "The Next Digital Divide: Online Social Network Privacy", March 2008, online: <http://www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_ Institute_OSN_Report.pdf>, at 11 [Digital Divide].

99 *Online Tracking*, *supra* note 26 at 17. The report goes on to note that these children "do not expect adults to be part of that public, even though they know that adults can see the information." (at 17).

100 Harvey Jones & José Hiram Soltren, "Facebook: Threats to Privacy", 15 December 2005, online: <http://www.swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf>.

101 Alberta *Regulation*, *supra* note 58, s. 7(e).

102 See BC *Regulation*, *supra* note 58, s. 6(1)(d).

the purposes for which it was made publicly available, and any such collection, use or disclosure must also be for purposes that a reasonable person would consider appropriate in the circumstances. These limitations are important in protecting individuals against inappropriate and unanticipated uses of their personal information by private sector organizations engaged in commercial activity.

With most of the categories of publicly available information, the purposes for which the information was made publicly available are relatively easy to discern. Telephone directory information is made available to provide contact information for the individuals whose names are included in the listings. Business or professional directory information is made available for similar purposes. Public registry information is made publicly available for purposes which are generally ascertainable from the enabling legislation or related policy documents. In the case of court or tribunal decisions, a number of purposes may be identified, but these are all *public* purposes, and would clearly not include profiling or marketing activities. The final category — that of "published information" — is the most challenging. Yet the examples of publications that are given in the section are newspapers, magazines and books — the dissemination of information in these vehicles is typically meant to educate or inform the public and serves a broader public interest.[103] In any event, the exception is only available where the individual is the immediate source of the information. Thus an element of consent is built into this exception — the individual must have consented to the original publication of the information. Further, any collection, use or disclosure of the information must be for the purposes for which it was published.

Expanding the scope of what is "publicly available information" to capture such things as activity in public view seems to equate "public" information with "publicly available" information. There is much information that is public, yet that is not excluded from the consent requirements of data protection legislation. While it is true that *Charter* cases and some tort cases draw distinctions between "private" and "public" information, this has never been the case in the data protection context. This is because the goal is to protect individuals from collection, use or disclosure of their personal information without their consent by organizations engaged in commercial activity. It generally does not matter if the information is "public" or "private" — the individual still has a right of control over the commercial exploitation of this information by others. Once broad categories of "public" information (information in public view) are exempted from the consent requirements for collection, use and disclosure, genuine data protection is lost. Austin cautions that "control over personal information will only provide illusory privacy protection if individuals are not given meaningful choices with respect to their information."[104]

In *United Food*, the issue faced by the court was whether the consent rules in PIPA — or the statute as a whole — should apply to information collected on a picket line in the course of a labour dispute. The court found a public interest in free expression in this context, and expressed concerns that data protection legislation might unduly limit the Union's expressive activities. As a result, one of the

---

103 See Scassa, "Journalistic Purposes", *supra* note 15.

104 Austin, *supra* note 28 at 25.

issues in the case was whether the exemptions for publicly available information should be expanded to capture information generally in public view.

It is important to note that expanding the scope of the publicly available information exception is not the only — nor is it necessarily the best — way to ensure that some personal information in public view can be collected, used or disclosed. Currently, the structure of PIPEDA gives scope for the collection, use or disclosure of personal information without consent in a range of contexts that depend not on the nature of the *source* of the information, but rather on the *purpose* for which it is being collected, used or disclosed. Thus, where information is being collected, used or disclosed in the context of an investigation, for national security purposes, pursuant to a court order, or for journalistic purposes, for example, exceptions to the consent rule already exist.[105] If there is a specific context in which Parliament considers that some personal information should be open to collection, use or disclosure without consent, this context can be added to section 7 of PIPEDA, without going so far as to create a new category of publicly available information. Thus, to use the example of *United Foods*, if Parliament or a provincial legislature considered it important that information relating to picket line activity be capable of collection, use or disclosure without consent, it could craft an exception to the rules of consent to address that context.

The exception for publicly available information is carefully limited by law to the collection, use and disclosure of personal information without consent only for purposes for which such information is made public. While purposes can be more or less ascertained with each of the current categories in the *Regulations*, it would be difficult to tell what any individual's purpose was in moving through public space, or in posting information to a social networking site. The purpose of a Facebook posting might be to share baby pictures with grandparents and other relatives; it might be to gain friends or increase one's status within one's peer group; it might be to promote one's career or professional profile. A recent Canadian study indicates that youth who post information on social networking sites conceive of three separate networks for their information — friends, family and work. The study suggests that these users of social networking sites expect these networks to remain separate, and are concerned "about the risk that their personal information, while quite freely shared and open to many within their network of friends, will end up in the hands of others, such as their family and managers, who may not be members of the same network."[106] Thus even when information is posted publicly, the person posting the information may have a preconceived expectation of who the public is for that information, and may have no intention of sharing that information with others. A report by the Office of the Privacy Commissioner of Canada indicates that "[y]oung adults are likely to post information that promotes the identity they want to project to the audience."[107] This makes determining the purpose

---

105 These are found in section 7 of PIPEDA, *supra* note 1.

106 Digital Divide, *supra* note 98 at 74. The recent report by the OPC on *Online Tracking*, *supra* note 26 at 17, echoes this point when it discusses the "invisible audience" that those who post information on social networks conceive of in making information available.

107 *Online Tracking*, *supra* note 26 at 17.

for which certain information is posted to social networking sites even more complex. Including information posted online within the categories of "publicly available information" would run counter to the expectations of many users of these sites, and it would become unwieldy because it would be difficult to know the purpose for which such information was provided.[108] The same is true for information about other general activities in public. Rather than expand the exception for publicly available information, it makes more sense to identify those contexts (such as picket line activity) that are judged to have sufficient public importance to warrant a specific exception to the rule of consent.

It should be noted as well that the fact that individuals have posted information to social networking sites or have carried out certain activities in public can also be taken into account under the existing data protection legislation without directly exempting this type of information from the rules of consent. The law already contemplates a kind of sliding scale for consent. Consent may be express or implied, it may be obtained by opt in or opt out methods. The type of consent required in any given case will depend on a range of circumstances. Key among these is the sensitivity of the information. Where information is of a less sensitive nature, the threshold for obtaining consent may be lower. It is certainly open to courts and adjudicators to determine that information that an individual has chosen to publish online in a relatively open context is of a less sensitive nature than other information. This does not obviate the need for consent; and indeed it is only one of the many contextual factors that must be taken into account. Such an approach, however, does more to preserve the delicate balance struck in data protection legislation than it does declaring open season on information individuals choose to share with others in online fora or that relates to their activities in public.

Finally, the relationship between PIPEDA and its substantially similar provincial counterparts must be kept in mind in considering reforms to PIPEDA or changes to its substantially similar counterparts. It can be confusing and disruptive to the smooth operation of commerce to have very different data protection norms or thresholds from one province to another. There are no doubt many ways that the statutes can be improved, reformed or amended that would not dramatically change their scope or their core normative principles.[109] However, a change to the regulations governing publicly available information that would include social networking sites or information revealed in public contexts would be significant, and would lead to this information being treated very differently in one jurisdiction than it is in another.

IV. CONCLUSION

Under the current structure of PIPEDA, consent is not required for the collection, use or disclosure of personal information that is "publicly available." The

---

108 Research carried out for the Office of the Privacy Commissioner of Canada indicates that most users of social networking sites in the target study group posted information primarily to share it with friends. (Decima Research, *supra* note 93 at 6).

109 For example, the manner in which PIPEDA is enforced, or the addition of a remedy for a data security breach, could be added without changing the core normative provisions of the legislation.

Regulations Specifying Publicly Available Information contain a closed list of sources of information that can be considered publicly available. The *Regulations* are drafted narrowly, and it is also clear that the exception to the rule of consent for "publicly available information" is available only where such information is collected, used or disclosed for the purposes for which it was made publicly available, or for purposes which a reasonable person would consider appropriate in the circumstances.

In *United Food*, the Alberta Court of Appeal suggests that the publicly available information exception may be unduly narrow because it does not capture information in public view. Yet such an approach would gut not only the carefully crafted and deliberately limited exception, it would eviscerate data protection law more generally. Public information is still personal information, and in the data protection context, the main objective is to provide individuals with some measure of control over the use of their personal information by private sector organizations.

Currently it might be possible to argue that some information posted on social networking sites or in other internet contexts by the data subject could fall within one of the existing categories of publicly available information. For example, information posted to a site such as LinkedIn might be argued to be information in a professional or business directory. Information posted on blogs or on a site such as Facebook might be argued to be a "publication." However, there are good reasons not to interpret these categories in the *Regulations* so broadly as to include all such sources of personal information. It is not clear that all social networking sites are genuinely "publicly available."

Rather than opening individuals' movements through public space (real or virtual) to unrestricted data harvesting, a better approach would be to consider whether the existing exceptions to consent set out in section 7 of PIPEDA are sufficient to meet the legitimate needs of businesses, and to satisfy the public interest. Currently these exceptions permit collection, use or disclosure of personal information for a wide range of purposes including debt collection, emergency situations, where there is a court order, or for investigations. If there is a specific context which is lacking from the list, it would be preferable to address that context, rather than to exempt an entire category of information from the fundamentally important requirement of consent for its collection, use or disclosure.