# PROMOTING TRANSPARENCY WHILE PROTECTING PRIVACY IN OPEN GOVERNMENT IN CANADA

AMY CONROY* AND TERESA SCASSA**

*The pressure towards open data and proactive disclosure by government in Canada has created a renewed need to balance the competing values of transparency and privacy. This article addresses issues such as what constitutes personal information and therefore engages privacy concerns, and whether transparency goals are actually met by disclosure in every case. The decision of the Supreme Court of Canada in* Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner) *addressed these types of issues in the access to information context and so offers some important insights. Finally, this article proposes some guiding principles to assist in striking a balance between transparency and privacy.*

## TABLE OF CONTENTS



## I. INTRODUCTION

Like other Western nations, Canada is rapidly moving into a new digital data environment in which many of the ways we conceive of privacy and access to government information will be transformed. The backdrop to this new environment is big data[1] analytics — the ongoing real time collection and use of vast amounts of data for profiling, targeting, predicting, analyzing, and conducting scientific research.[2] This data revolution is complex

* Doctoral Student, Faculty of Law, University of Ottawa.
** Canada Research Chair in Information Law, Faculty of Law, University of Ottawa. The authors gratefully acknowledge the support of the Social Sciences and Humanities Research Council of Canada for the Geothink project, of which this research is a part.

1 "Big data" has been defined as "data linked together, to create a digital picture that is bigger than the sum of the parts" (Andy Williamson, "Big Data and the Implications for Government" (2014) 14:4 Leg Info Mgmt 253 at 253). It is also often explained in relation to three main concepts: volume, velocity, and variety (see e.g. Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences* (London: Sage, 2014) at 68 [Kitchin, *Data Revolution*]).

2 The data analytics movement has brought on questions about how to manage huge amounts of data as well as concerns about data quality and usability that are explored in this paper. See discussion in Rob Kitchin & Tracey P Lauriault, "Towards critical data studies: Charting and unpacking data assemblages and their work" (2014) The Programmable City Working Paper No 2, online: <papers.ssrn.com/sol3/papers.cfm?abstract_id=2474112>.

and multi-faceted.[3] The engines of big data are fuelled by data from a broad range of sources, one of which is government.[4]

Governments in Canada are facing increasing pressure to conform to two relatively new approaches to government data and information: proactive disclosure and open data. Both form part of the growing open government movement — a movement which pushes for the greater release of government information and data in the name of increased transparency and accountability.[5] Both open data and the proactive disclosure of government information are seen as important new means by which governments can meet these goals.[6] At the same time, open data is also touted as a means by which to drive innovation in the knowledge and information economies.[7]

This article considers the potential impacts on citizen privacy of the drive towards open data and proactive disclosure of government information. It necessarily does so within a context in which data from all sources — including government — fuels the engines of big data analytics. Since this article considers privacy in the context of the release of government information, and since the move towards open data and the proactive disclosure of information in Canada is taking place in the absence of any new legislative frameworks, these issues are considered within the context of the existing access to information and public sector privacy frameworks. The recent Supreme Court of Canada decision in *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)* is used as a departure point.[8] Although it did not specifically address either open data or proactive disclosure, this case, which resulted in the disclosure of certain government information, and which was hailed as a "victory for openness and transparency,"[9] offers some important insights into the lacunae of legislation and case law in this area.

---

3 Kitchin, *Data Revolution*, *supra* note 1.

4 *Ibid* at 113-27; Rhoda C Joseph & Norman A Johnson, "Big Data and Transformational Government" (2013) 15:6 IT Professional 43; Williamson, *supra* note 1 at 253–57.

5 Patrice McDermott, "Building Open Government" (2010) 27:4 Government Information Q 401; Angela M Evans & Adriana Campos, "Open Government Initiatives: Challenges of Citizen Participation" (2013) 32:1 J Policy Analysis & Management 172 at 173; Aikaterini Yannoukakou & Iliana Araka, "Access to Government Information: Right to Information and Open Government Data Synergy" (2014) 147 Procedia Social & Behavioral Sciences 332 at 333; Katleen Janssen, "Open Government Data and the Right to Information: Opportunities and Obstacles" (2012) 8:2 J Community Informatics [Janssen, "Open Government"].

6 Treasury Board of Canada Secretariat, "Canada's Action Plan on Open Government 2014-16," Catalogue No BT22-130/2014E-PDF (Ottawa: TBCS, 2014) ["Canada's Action Plan"], online: <publications.gc.ca/collections/collection_2014/sct-tbs/BT220130-2014-eng.pdf>; Canada, "Open Government," online: <open.canada.ca/en>.

7 Canada, "G8 Open Data Charter — Canada's Action Plan," online: <open.canada.ca/en/g8-open-data-charter-canadas-action-plan> ["G8 Open Data"]; Janssen, "Open Government," *supra* note 5; James Manyika et al, *Big Data: The next frontier for innovation, competition and productivity*, Report by the McKinsey Global Institute (McKinsey & Co, 2011), online: <www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation>; James Vincent, "G8 Open Data Charter will 'increase transparency' and 'fuel innovation,'" *The Independent* (19 June 2013), online: <www.independent.co.uk/life-style/gadgets-and-tech/g8-open-data-charter-will-increase-transparency-and-fuel-innovation-8665696.html>.

8 2014 SCC 31, [2014] 1 SCR 674 [*Community Safety and Correctional Services*].

9 See comments by former Information and Privacy Commissioner of Ontario Ann Cavoukian: OIPC, Press Release, "A Victory for Openness and Transparency: The Supreme Court of Canada Supports the Public's Right to Know" (28 April 2014), online: CNW Group <www.newswire.ca/ news-releases/a-victory-for-openness-and-transparency-the-supreme-court-of-canada-supports-the-publics-right-to-know-514164211.html> [OIPC, "Victory"].

In particular, this article examines three issues arising from the decision in *Community Safety and Correctional Services* and considers each issue against the twin principles of privacy and transparency that underlie the access to information legislation against which this case was decided. The first relates to the implications of the decision for the privacy of personal information in the hands of government. A key factor in any decision to disclose information is the determination of whether that information is personal information within the meaning of the legislation. Since there are no clear and unequivocal markers for personal information, the approach of the courts to determining when something is personal information is crucial and has a direct impact on how the balance between transparency and privacy is struck.

The second issue raised by *Community Safety and Correctional Services* relates to how adjudicators understand transparency in the face of competing claims such as privacy. In this case we argue that the Ontario Information and Privacy Commissioner's (OIPC) claim that the decision represents a win for transparency is problematic, given the lack of a clear assessment of either the scope of the transparency principle or the extent to which disclosure in this case actually serves transparency goals. This article considers the meaning of transparency, its relationship to data quality, and the ease with which the limitations of any data set can be assessed. We suggest that it may be a fallacy simply to equate transparency with disclosure, and that true transparency may require additional steps.

Finally, the article examines how best to strike the balance between transparency on the one hand and privacy on the other. This issue is poised to become crucial as governments at all levels in Canada move towards both proactive disclosure of government information[10] and open data.[11] It is argued in this article that the balance endorsed by the Supreme Court of Canada in *Community Safety and Correctional Services* results in a slant towards promoting transparency in government over the protection of personal information in the long-term. We consider whether this reflects a carefully considered public policy position within our contemporary data context or whether it reflects a balancing of transparency and privacy values based upon an information environment that is now obsolete. The article concludes by identifying some guiding principles for balancing transparency and privacy, not just in the context of access to information requests, but in the rapidly evolving contexts of open government data and proactive disclosure of government information.

Before examining these three issues, it is useful to define certain key concepts for the discussion that follows. The concept of transparency is described at length after a review of the decision in *Community Safety and Correctional Services* and as part of the second aim

---

[10] At the federal level, see "Canada's Action Plan," *supra* note 6. At the provincial level, British Columbia, Alberta, Ontario, Quebec, and Newfoundland are already actively engaged in the open government movement: see Alberta, "Alberta Open Data," online: <data.alberta.ca>; British Columbia, "DataBC," online: <www.data.gov.bc.ca>; Ontario, "Open Data," online: <www.ontario.ca/government/government-ontario-open-data>; Newfoundland and Labrador, "Open Government," online: <www.open.gov.nl.ca>; Quebec, "Données Ouvertes," online: <donnees.gouv.qc.ca/?node=/accueil>.

[11] See the federal government's announcement of the pan-Canadian open data strategy, "Open Data Canada" ("G8 Open Data," *supra* note 7). For information on the numerous provinces and municipalities that have adopted their own open data strategies, see Canada, "Open Government Across Canada," online: <open.Canada.ca/en/maps/open-data-canada>; Datalibre.ca, "Open Data," online: <datalibre.ca/links-resources/> [Datalibre] (which lists 55 (mostly government-led with some citizen-led) open data initiatives at the city level).

described above. Other key terms include open access, a notion that is linked to the right to information movement. This right has primarily been implemented by access to information frameworks where individual requests for government-held information can be made.[12] Proactive disclosure involves the proactive release of government-held information with a view to respecting open access principles while also increasing transparency, citizen engagement, innovation, and economic growth.[13] There is thus an important distinction between proactive disclosure of information, which refers to "steps public bodies take to provide information to the public on their own accord"[14] and access to information principles, which require the government to "provid[e] information only when responding to a freedom of information request."[15] Proactive release of information describes a "push" rather than a "pull" approach to access to information in the hands of government.[16] The purposes of both proactive release of information and access to information principles are related, as both aim to serve the public's right to information. However, open data and proactive disclosure also work to fulfill, on a broad scale, the additional goals noted above. Likewise, access to information schemes serve some more specific goals not encompassed by the open data and proactive disclosure movements. For instance, access to information requests will continue to require the government to respond to public demands for information that is not proactively disclosed or for information that constitutes personal information belonging to the requester.[17] Thus, while the proactive release of information is likely to decrease the number of access to information requests, the access to information schemes that have traditionally served open access principles will continue to play a distinct and important role in this environment.[18]

Open data is an element of open government, and involves the provision of government data sets in reusable formats according to open standards.[19] Open data can be achieved through proactive release of information in the open government context and is therefore linked to the open government movement. However, it involves more than mere proactive disclosure of information and requires that data be released in reusable electronic formats

---

12 Teresa Scassa, "Privacy and Open Government" (2014) 6:2 Future Internet 397 at 399 [Scassa, "Privacy"]; Treasury Board of Canada Secretariat, "Canada's Action Plan on Open Government," Catalogue No BT22-130/2012E-PDF (Ottawa: TBCS, 2012), online: <publications.gc.ca/site/eng/9.696071/publication.html> at 1 (emphasizing "open access to public sector information and data and, in particular, the need to improve the availability of data to researchers and the private sector with fewer restrictions on reuse of these information assets").

13 Katleen Janssen, "Open Government Data: Right to Information 2.0 or its Rollback Version?" (2012) Interdisciplinary Centre for Law and ICT, ICRI Working Paper No 8/2012, online: <papers.ssrn.com/sol3/papers.cfm?abstract_id=2152566>; Janssen, "Open Government," *supra* note 5.

14 British Columbia, Information and Privacy Commissioner, "Investigation into the Simultaneous Disclosure Practice of BC Ferries," by Elizabeth Denham, Investigation Report No F11-02 (Victoria: BCIPC, 16 May 2011) at para 3.

15 *Ibid*.

16 The movement towards the more proactive release of publicly-held information has led to the creation of a Government of Canada webpage providing access to the numerous proactive disclosure pages of the individual departments: see e.g. Treasury Board of Canada Secretariat, "Government-Wide Reporting — Proactive Disclosure," online: <www.tbs-sct.gc.ca/pd-dp/gr-rg/index-eng.asp>; Canada, Legal and Legislative Affairs Division, Parliamentary Information and Research Service, "Government 2.0 and Access to Information: 1. Recent Developments in Proactive Disclosure and Open Data in Canada," by Alysia Davies & Dara Lithwick, Publication No 2010-14-E (Ottawa: Parliamentary Information and Research Service, 15 April 2010) (describing the proactive disclosure movements at the municipal, provincial, and federal levels in Canada).

17 Scassa, "Privacy," *supra* note 12 at 399.

18 *Ibid*.

19 *Ibid*; "Canada's Action Plan," *supra* note 6.

under an open licence for reuse.[20] It is through this additional requirement that open data principles serve the goals of innovation and economic development, in addition to the values of transparency and accountability in government. Open data sets are explicitly not meant to contain personal information.[21] High-value open data may include geospatial data sets and geodemographic information, but can also include a broad range of government information such as transit timetable data, weather, and other environmental data.

The issues discussed in this article all relate to its core theme: the need to recalibrate the balance between privacy and transparency in the release of government information in the contemporary big data environment. Paul Ohm has argued that "[b]efore enacting any privacy law, lawmakers should weigh the benefits of unfettered information flow against its costs and must calibrate new laws to impose burdens only when they outweigh the harms the laws help avoid."[22] This underlines the need to understand and acknowledge the risks on both ends of the privacy-transparency spectrum. Therefore, in the interest of achieving balance, limits on disclosure of some government-held information may be required.[23] At the same time, in certain cases, personal privacy interests will need to yield to group interests, including greater transparency in the public sector.[24] Our analysis of the Supreme Court of Canada's decision in *Community Safety and Correctional Services* provides a backdrop for elaborating on the concept of transparency and its relationship with personal privacy, not just in the access to information context in which it arose, but also in the growing open data and open government movements.

## II. TRANSPARENCY AND PRIVACY IN THE ACCESS TO INFORMATION PARADIGM

On 24 April 2014, the Supreme Court of Canada released its decision in *Community Safety and Correctional Services*.[25] The case arose from a dispute between the Ministry of Community Safety and Correctional Services (the Ministry) and a journalist following the latter's request to the Ministry for disclosure of "an electronic copy of the Ontario sex offender registry, edited in such a way as to show only the first three characters of the holder's postal code (eg. M6G)."[26] The Ontario Sex Offender Registry (OSOR) which has been in operation since 2001, was established by *Christopher's Law*,[27] named after 11-year-

---

20 Scassa, "Privacy," *ibid*.

21 See "G8 Open Data," *supra* note 7 (explaining that the Government of Canada will facilitate open data while continuing to safeguard privacy by restricting the release of information for privacy and confidentiality purposes). See also City of Vancouver, "Open Data Catalogue," online: <vancouver.ca/your-government/open-data-catalogue.aspx> (defining open and accessible data as "non-personally identifiable data that is made freely available to everyone in one or more open and accessible formats").

22 Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57:6 UCLA L Rev 1701 at 1736.

23 Scassa, "Privacy," *supra* note 12 at 404.

24 *Ibid* at 405.

25 *Supra* note 8.

26 *Re Ministry of Community Safety and Correctional Services* (2009), Order PO-2811, Appeal PA09-213-2 (OIPC) at 1 [*Community Safety* OIPC]. The requester has since explained that his initial request for the information was purposely limited to the first three letters of offenders' postal codes, based on the assumption that, at this level of specificity, the data would be considered mere "generic statistical information" (Patrick Cain, "Today's Supreme Court case on sex offender data: the back story" *Global News* (5 December 2013), online: <globalnews.ca/news/1011601/todays-supreme-court-case-on-sex-offender-data-the-back-story/>).

27 *Christopher's Law (Sex Offender Registry)*, SO 2000, c 1 [*Christopher's Law*].

old Christopher Stephenson, who was tragically sexually assaulted and murdered in 1988.[28] *Christopher's Law* authorizes the Ministry to collect and record the names, dates of birth, current addresses, and a photograph of adults convicted of designated sexual offences or charged with such offences but found not criminally responsible. The information is accompanied by details of the sex crimes that each offender has committed.[29] Young offenders are only included if they are tried or convicted as adults.[30] Offenders are required to keep the Ministry updated on their place of residence by reporting annually to their local police and notifying police within 15 days of a change of residence or of any intent to become resident of or cease to reside within the province of Ontario.[31]

In *Community Safety and Correctional Services*, the journalist's request for the information was made under the *Freedom of Information and Protection of Privacy Act*,[32] which provides for a right of access to information under the control of a public institution unless one of the specific exceptions outlined within the *Act* applies to the circumstances. Finding that no relevant exception justified the withholding of the information in this case, the adjudicator who first heard the dispute in court ordered the release of the information — this decision was upheld on appeal all the way to the Supreme Court of Canada.[33] Using the information disclosed pursuant to that order, a map was created and published online by *Global News*. The map purports to provide a visual representation of the whereabouts of registered sex offenders per "Forward Sortation Areas" (FSAs) in Ontario.[34] Prior to the release of this map, the information contained in the OSOR had never been made available to the public.[35] The Ontario government has explained that this policy is in place because it

---

28 Christopher was abducted from outside a shopping mall. His body was found two days later. The perpetrator was a previously convicted sex offender who was on parole at the time of the assault and murder. An inquiry into the circumstances of the boy's death concluded that there was a need for a registry for convicted, dangerous, high-risk sexual offenders. The OSOR was developed as the first of two sex offender registries operating in Canada, the other being the National Sex Offender Registry (NSOR), which is separately maintained in accordance with the *Sex Offender Information Registration Act*, SC 2004, c 10. The OSOR was the first registry of its kind in Canada, and was established before the federal government acted to create a national registry. The NSOR was created after several other provinces voiced intentions to create provincial registries, forcing the federal government into action. See Ontario, Ministry of Community Safety & Correctional Services, "Policing Services: Ontario Sex Offender Registry," online: <www.mcscs.jus.gov.on.ca/english/police_serv/sor/ChristophersLaw/sor.html> ["Policing Services, OSOR"]; Lisa Murphy, J Paul Fedoroff & Melissa Martineau, "Canada's sex offender registries: Background, implementation, and social policy considerations" (2009) 18:1–2 Can J Human Sexuality 61 at 62–63.

29 *Supra* note 27, s 2.

30 *Ibid*, s 8(2)–(3).

31 *Ibid*, s 3.

32 RSO 1990, c F.31 [*FOIPP* (ON)].

33 *Community Safety* OIPC, *supra* note 26 at 17; *Community Safety and Correctional Services*, *supra* note 8.

34 Patrick Cain, "Updated: Here's the sex offender map Ontario didn't want you to see," *Global News* (9 June 2014), online: <globalnews.ca/news/1313399/heres-the-sex-offender-map-ontario-didnt-want-you-to-see/> [Cain, "Sex Offender Map"].

35 This is in contrast to the general position taken in the United States. President George W Bush's government was active in the movement to increase access to information about the whereabouts of registered sex offenders and created a publicly accessible online forum to share this information across state lines: see US Department of Justice, "Dru Sjodin National Sex Offender Public Website," online: <www.nsopw.gov/en>). Like the OSOR, the information on the NSOR is not currently shared with the public, however the Conservative government has introduced a bill to allow public sharing of this information as part of its tough on crime agenda. The government has also proposed a national public registry for high-risk child sex offenders: see Amanda Connolly, "Public sex offender registry coming soon, says Peter MacKay," *CBC News* (28 February 2014), online: <www.cbc.ca/news/canada/calgary/public-sex-offender-registry-coming-soon-says-peter-mackay-1.2556080>; Canada, Royal Canadian Mounted Police, "National Sex Offender Registry" (Ottawa: RCMP, 2015), online: <www.rcmp-grc.gc.ca/tops-opst/bs-sc/nsor-rnds/index-eng.htm>. In addition to privacy concerns, there are concerns over vigilantism, which has already been facilitated in the US through publicly available sex offender

"contributes to a consistently high offender compliance rate resulting in increased accuracy and integrity of the data on the OSOR," which in turn facilitates the primary purposes of the registry, being to assist with police investigations and to prevent crime.[36] The order for release of the information therefore led to the first public glimpse of the information contained in the OSOR.

There are different views of what the conflicting public policy issues are that underlie the decision of the Supreme Court of Canada in this case. Ontario's Information and Privacy Commissioner at the time, Ann Cavoukian, responded to the Supreme Court's decision, emphasizing that the ruling "wasn't a privacy issue.… It was an issue of government transparency. This [information] should be made available to the public. That's what freedom of information is all about."[37] Elsewhere she clarified, however, that the decision could be expected to have benefits for both underlying goals in that it represents "a vote in favour of transparency, and, in turn, privacy."[38] The Ministry, on the other hand, viewed the dispute as a law enforcement concern and a matter of public safety in which personal privacy played a central role, and tried unsuccessfully to establish that this was an appropriate case for application of the personal privacy and law enforcement exceptions provided for in Ontario's *FOIPP* legislation. The case highlights the tension between the goal of transparency in government and the need to protect individual privacy, two objectives that underlie access to information legislation.[39] We further argue that it highlights challenges that will become increasingly important as governments at all levels move towards proactive disclosure of government information and open data.

Although this litigation originated in the mid-2000s, well before the current shift in Canada towards open data and proactive disclosure of government information, the decisions of the OIPC and the courts in this case reveal important issues regarding how the goals of government transparency, on the one hand, and personal privacy on the other, should be managed in these new contexts.[40] In spite of the dramatically changing landscape for disclosure of government data at all levels of government in Canada, the decision of the

---

registry information. See e.g. the story of a Nova Scotia man who tracked down two sex offenders in Maine after accessing the state's public registry. He shot and killed both men before committing suicide ("Maine murders baffle police," *CBC News* (21 April 2006), online: <www.cbc.ca/ news/canada/nova-scotia/maine-murders-baffle-police-1.579331> ["Maine Murders Baffle Police"].

36 "Policing Services, OSOR," *supra* note 28. The purpose of the OSOR is outlined in the preamble of *Christopher's Law*, *supra* note 27, which states:

> The people of Ontario believe that there is a need to ensure the safety and security of all persons in Ontario and that police forces require access to information about the whereabouts of sex offenders in order to assist them in the important work of maintaining community safety. The people of Ontario further believe that a registry of sex offenders will provide the information and investigative tools that their police forces require in order to prevent and solve crimes of a sexual nature.

Statistics indeed show a lower rate of compliance that is directly linked to registries being open for public access (Murphy, Fedoroff & Martineau, *supra* note 28 at 68). The Ontario courts have acknowledged that the confidentiality provisions in the OSOR scheme have resulted in higher compliance rates than those seen in American jurisdictions: see *R v Dyck*, 2008 ONCA 309, 90 OR (3d) 409 at para 25.

37 Don Butler, "Release of sex offender data hailed as victory for transparency" *Ottawa Citizen* (25 April 2014), online: <ottawacitizen.com/news/local-news/release-of-sex-offender-data-hailed-as-victory-for-transparency>.

38 OIPC, "Victory," *supra* note 9.

39 In the case of Ontario's legislation, see Christopher Berzins, "Ontario's Freedom of Information and Protection of Privacy Act After 25 Years: A Critical Assessment" (2014) 43:1 Adv Q 80.

40 Regarding the *FOIPP* (ON), Berzins, *ibid* at 87–88, noted that the *Act* is not only poorly drafted, but is not well adapted to issues related to the release of information in electronic formats.

Supreme Court of Canada rests comfortably within an earlier government information paradigm. Although both the open data movement and the drive towards proactive disclosure of government data share the goals of transparency and accountability that are fostered by freedom of information legislation, both proactive disclosure and open data serve other goals as well.[41] The breadth and volume of data that will ultimately be disclosed through government data portals in Canada — and into our contemporary big data environment[42] — requires a re-examination of how the balance between transparency and privacy is struck. The goal of transparency, in and of itself, is not explicitly defined or explained in Ontario's *FOIPP*. Instead, the *Act* sets out the principle that information under the control of government institutions "should be available to the public" and that "necessary exemptions from the right of access should be limited and specific."[43] While transparency and accountability may be the underlying principles, the legislated norm is broader and less specific. It is simply public availability. Significantly, the law also establishes the free-standing obligation "to protect the privacy of individuals with respect to personal information about themselves held by institutions."[44] The two, then, are distinct principles embedded in the legislation.[45] Privacy is not simply one of the specific and limited exceptions to the broader rule of disclosure.

These twin principles are framed in similar ways in other provincial statutes — establishing both an access right and the obligation to protect citizen privacy.[46] British Columbia's legislation is particularly interesting. Not only does it identify accountability as a governing principle,[47] it sets out a right of access counterbalanced by privacy considerations, and then states that the legislation does not "limit in any way access to information that is not personal information and is available to the public."[48] The federal *Access to Information Act*[49] does not make explicit reference to privacy in its statement of purpose. Rather, it states that it provides for access in accordance with the "principles that government information should be available to the public, [and] that necessary exceptions to the right of access should be limited and specific."[50] However, the lack of reference to privacy should be understood in the specific context of this statute. Under the federal scheme,

---

41 Additional goals served by these movements are more public participation in government affairs, general economic development, cost-savings in research, and support for innovative uses of information: see Scassa, "Privacy," *supra* note 12 at 397; Anneke Zuiderwijk & Marijn Janssen, "Open data policies, their implementation and impact: A framework for comparison" (2014) 31:1 Government Information Q 17 at 17; Marijn Janssen, Yannis Charalabidis & Anneke Zuiderwijk, "Benefits, Adoption Barriers and Myths of Open Data and Open Government" (2012) 29:4 Information Systems Management 258 at 260–61; "G8 Open Data," *supra* note 7; Open Government Partnership, "Open Government Declaration," online: <www.opengovpartnership.org/about/open-government-declaration>.

42 For examples of data already disclosed in this environment, see Canada, "Open Government," *supra* note 6. See again the numerous open data initiatives listed by Datalibre.ca, *supra* note 11.

43 *FOIPP* (ON), *supra* note 32, s 1(a).

44 *Ibid*, s 1(b).

45 See the discussion in Berzins, *supra* note 39 at 88, noting the "asymmetry between the provisions governing access to information and those dealing with the protection of personal information" with respect to *FOIPP* (ON), *ibid*.

46 Note, however, that in some cases, the right of access may be framed more narrowly. For example, in Manitoba, the *Freedom of Information and Protection of Privacy Act*, SM 2008, c 40, CCSM, c F175, s 2(a) provides for "a right of access to records in the custody or under the control of public bodies," rather than the more open-ended concept of "availability" present in the Ontario legislation (*FOIPP* (ON), *ibid*, s 1).

47 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, s 2(1) [*FOIPP* (BC)].

48 *Ibid*, s 2(2).

49 RSC 1985, c A-1.

50 *Ibid*, s 2(1).

the government's privacy obligations are dealt with under the *Privacy Act*,[51] and different independent commissioners oversee each statute. Nevertheless, the *Access to Information Act* clearly limits access based on privacy considerations.[52] Like the British Columbia statute, the federal statute also states that it "is not intended to limit in any way access to the type of government information that is normally available to the general public."[53] It is worth noting that, as open data programs and proactive disclosure agendas expand, the range of government information "normally available to the general public" will also continue to expand.[54]

It is clear that providing access to government information and protecting the privacy of personal information in the hands of government are principles that are closely linked at all levels of government in Canada. Privacy is not only a key limiting factor in access requests, constituting a part of the limited and specific exceptions to the right of access, it is also a separate and freestanding obligation of government, and a right held by individuals.[55]

## III. PRIVACY AND THE DEFINITION OF PERSONAL INFORMATION

Governments at all levels in Canada have an obligation to protect the information they receive from members of the public. These obligations are found in the statutory limits on collection, management, retention, and use of personal information.[56] Access to information regimes also place limits on the ability of governments to disclose the personal information of individuals.[57] Within this framework, the definition of personal information is crucial. It effectively draws the line between what the government is obliged to protect, and that which the government may share more broadly.

Privacy is a fundamental value. Indeed the Supreme Court of Canada has described privacy legislation as being quasi-constitutional in nature, and has confirmed that the protection of privacy enhances human dignity and autonomy.[58] Privacy rights are given constitutional protection from interference by government under the *Canadian Charter of Rights and Freedoms*.[59] The Quebec *Charter of Human Rights and Freedoms*[60] also recognizes privacy as a human right and social value. Public sector privacy legislation in Canada recognizes the rights of individuals to have their personal information in the hands

---

51 RSC 1985, c P-21.

52 *Supra* note 49, s 19.

53 *Ibid*, s 2(2).

54 The federal government's plans for expanding both its open data offerings and for moving towards proactive disclosure can be found in "Canada's Action Plan," *supra* note 6.

55 See e.g. *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 SCR 733 at para 19 [*United Food*]; *Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, [2002] 2 SCR 773 at para 24 [*Lavigne*]; *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at paras 65-66 [*Dagg*]; *HJ Heinz Co of Canada Ltd v Canada (Attorney General)*, 2006 SCC 13, [2006] 1 SCR 441 at para 28 [*Heinz*].

56 See e.g. *Privacy Act*, *supra* note 51, ss 4, 6(1), 7; *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25, ss 33, 35 [*FOIPP* (AB)]; *FOIPP* (BC), *supra* note 47, ss 26, 31–32; *FOIPP* (ON), *supra* note 32, ss 38(2), 40–41.

57 See e.g. *Access to Information Act*, supra note 49, s 19; *FOIPP* (AB), *ibid*, s 12(2)(b); *FOIPP* (BC), *ibid*, ss 33–33.3; *FOIPP* (ON), *ibid*, s 21.

58 See again *United Food*, *supra* note 55 at para 19, citing *Lavigne*, *supra* note 55 at para 24; *Dagg*, *supra* note 55 at paras 65–66; *Heinz*, *supra* note 55 at para 28.

59 Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

60 CQLR c C-12, s 5.

of government protected, and the corresponding obligations on governments to protect this information.[61]

The term "personal information" — used in both public and private sector data protection statutes in Canada — serves as a trigger for the application of the legislative protections. If information is not personal information (not information "about an identifiable individual"[62]) then no privacy right is engaged, and the government has no obligation to protect the privacy of the information at issue. In this context, a central question is not just how "personal information" is defined, but how this definition is applied. This is particularly the case with information that is not identifying on its own, but that when combined with other information, may lead to the identification of an individual or individuals. This application is critical to how transparency and privacy are balanced. A more restrictive approach to the definition will exclude more information from the category of "personal information," thus favouring transparency, whereas a more expansive approach to the definition of "personal information" will expand the scope of privacy protection by limiting the disclosure of certain kinds of information.[63]

Whether the sex offender data sought by the journalist in *Community Safety and Correctional Services* was personal information was a key issue in the Court's decision. By the time the case reached the Supreme Court of Canada, the Ministry had abandoned its argument relating to the privacy exemption on the basis that the protection of privacy of convicted sex offenders is not part of the primary purpose of the confidentiality provisions in *Christopher's Law*.[64] Nevertheless, the definition of personal information remained an underlying theme in the appeal. Although the issues in the case were reformulated by the time the dispute came before the Supreme Court of Canada, the focus on the interdependent issues relating to the personal privacy exemption, the definition of personal information, and the concept of identifiability remained relevant at all levels of the case.

When the dispute first came before the adjudicator for the OIPC, the question was whether the information requested by the journalist was exempt from disclosure under any of the following three sections of the *FOIPP* (ON):

---

61 See e.g. *Privacy Act*, *supra* note 51, s 2, which explains that the purpose of the Act is to "extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information." At the provincial level, see e.g. *FOIPP* (AB), *supra* note 56, s 2; *FOIPP* (BC), *supra* note 47, s 2; *FOIPP* (ON), *supra* note 32, s 1.

62 This is the definition that is generally given for personal information in Canada's privacy and access to information laws. See e.g. the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 2 [*PIPEDA*]; *Privacy Act*, *ibid*, s 3. See also the discussion in Teresa Scassa, Jennifer A Chandler & Elizabeth F Judge, "Privacy by the Wayside: The New Information Superhighway, Data Privacy, and the Deployment of Intelligent Transportation Systems" (2011) 74:1 Sask L Rev 117 at 138.

63 See Teresa Scassa, "Geographical Information as 'Personal Information'" (2010) 10:2 OUCJL 185 at 205 [Scassa, "Geographical Information"], discussing how public sector data protection legislation aims to balance broad public interests such as transparency and accountability in government against individual privacy. See also Stefan Kulk & Bastiaan van Loenen, "Brave New Open Data World?" (2012) 7 Intl J Spatial Data Infrastructures Research 196 at 196, discussing the fact that open data policies may lead to greater transparency in government, but may also be in conflict with individual privacy rights as prescribed by the European Union's Data Protection Directive.

64 *Community Safety and Correctional Services*, *supra* note 8 (Factum of the Appellant at para 20), online: <www.scc-csc.gc.ca/WebDocuments-DocumentsWeb/34949/FM010_Apellant_Ministry_of_Community_Safety_and_Correctional_Services.pdf> [Factum of the Appellant].

(1) Section 21(1): the "personal privacy exemption" which allows for information to be withheld if it qualifies as "personal information";

(2) Section 14(1)(e): the first of the "law enforcement exemptions" which provides that information may be withheld if its disclosure could reasonably be expected to "endanger the life or physical safety of a law enforcement officer or any other person"; or

(3) Section 14(1)(l): the second of the "law enforcement exemptions" which provides that information may be withheld if its release could reasonably be expected to "facilitate the commission of an unlawful act or hamper the control of crime."

The first exemption presented a direct question as to the definition of personal information under *FOIPP* (ON) since it required that the adjudicator determine whether the information at issue was "personal information" under section 2(1) of the *Act*.[65] The adjudicator noted that the requirement that information "be linked to an *identifiable* individual … is the hallmark of personal information as defined in the *Act*."[66] He turned to the leading test on identifiability in Ontario, *Ontario (AG) v. Pascoe,* which asks whether there is a reasonable expectation that an individual may be identified upon disclosure of the information.[67] Using the *Pascoe* test, the adjudicator considered the Ministry's argument regarding the risk of identifiability with respect to the information requested by the journalist in the case at hand.[68]

The Ministry argued that the disclosure of the number of registered sex offenders within each of the requested FSAs would constitute disclosure of personal information of sex offenders registered on the OSOR because the information could be combined with other publicly available information sources to identify the addresses of such individuals.[69] The Ministry cited examples of publicly available sources that might lead to this outcome, including information available through "the internet, newspapers, voter registration lists, occupational licensing registries, property records, crime/court records, corporate proxy statements, stock holding reports, city directories, birth, death, and marriage records."[70] The public availability of these sources of data was the basis for the Ministry's argument that

---

65 *Community Safety* OIPC, *supra* note 26 at 5.

66 *Ibid* at 7 [emphasis in original]. See discussion of "personal information" in Scassa, "Geographical Information," *supra* note 63.

67 (2002), 66 OAC 88 at para 1 (CA) [*Pascoe*]. This is the leading decision on "identifiability" in Ontario and the test has been applied in numerous tribunals and court decisions: see e.g. *Ministry of Correctional Services v Goodis* (2008), 89 OR (3d) 457 at para 69 (Sup Ct J); *Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157, [2007] 1 FCR 203 at para 43; *Re Ontario (Energy Board)* (2006), Order PO-2536, Appeal PA-060066-1 (OIPC) at 21; *Re Ontario (Community Safety and Correctional Services)* (2006), Order PO-2456, Appeal PA-040268-2 (OIPC) at 3; *Re Ontario (Community Safety and Correctional Services)* (2006), Order PO-2518, Appeal PA-030365-2, PA-040280-1, PA-030407-3 (OIPC) at 3; *Community Safety* OIPC, *supra* note 26 at 6. It has also been adopted in relation to provincial legislation outside of Ontario; in British Columbia, *Re British Columbia (Health Services)* (2003), Order 03-42 (BC IPC) at 5; *Re Eastern Regional Integrated Health Authority* (2007), Report 2007-008 (NL IPC) at para 7; *Re Workers Compensation Appeal Tribunal* (2005), Order 05-005 (PEI IPC) at 9; *Re Saskatchewan (Regina Qu'Appelle Regional Health Authority)* (2013), Review Report LA-2013-001 (Sask IPC) at para 57.

68 The *Pascoe* standard has been criticized for failing to identify the point of view from which reasonableness should be assessed. See e.g. Scassa, "Geographical Information," *supra* note 63 at 200; Khaled El Emam & Patricia Kosseim,"Privacy Interests in Prescription Data, Part 2" (2009) 7:2 IEEE Security & Privacy 75 at 75.

69 *Community Safety* OIPC, *supra* note 26 at 7.

70 *Ibid*.

there existed a reasonable expectation that an individual might be identified upon disclosure of the FSA information of those registered on the OSOR.

The adjudicator decided that combining the above sources of information with knowledge of the number of sex offenders residing within a given FSA could not reasonably be expected to reveal the identities of offenders registered on the OSOR.[71] This determination was largely based on the fact that the smallest number of individuals residing in an Ontario FSA was 396, with the average being over 24,000.[72] As the adjudicator found no reasonable expectation of identifiability on the facts, the information requested by the journalist was determined not to be personal information under section 2(1), which meant that the personal privacy exception under section 21(1) was inapplicable to the request in this case.[73]

Although this ended the inquiry on the section 21(1) claim, the decision that the requested information was not personal information impacted the decisions on each of the law enforcement exemptions. Under section 14(1)(e), the Ministry argued that the information should be exempt from disclosure because of the risk of harm to four groups of people: (1) the offenders themselves, who may be targeted by vigilantism if publicly identified; (2) the families and friends of offenders, who may become victims of harassment upon identification of the offender; (3) persons mistakenly identified as sex offenders; and (4) future victims of assaults that may result from offenders going underground out of fear of being identified and being without vital support from professionals, which would increase the likelihood that they might reoffend and generally impede the public safety mandate of the registry.[74] This risk of recidivism was also argued under section 14(1)(l), which allows for information to be exempted where its release could reasonably be expected to facilitate the commission of an unlawful act or hamper the control of crime.[75] Finding that all arguments made by the Ministry under sections 14(1)(e) and 14(1)(l) were dependent on individual concerns about the possibility of being identified (or in the case of mistaken identity, the assumption of identification), the adjudicator rejected the application of both sections to the facts of the case and ordered the release of the information.[76]

The adjudicator's decision was upheld on judicial review, and again upheld by the Court of Appeal before it came before the Supreme Court of Canada.[77] In the final appeal, the questions had been reformulated to reflect the following issues:

(1) The standard of review to be applied to the IPC's decision;

(2) whether the adjudicator made a reviewable error by granting access to the information for purposes inconsistent with *FOIPP* (ON) or *Christopher's Law*; and

---

71 *Ibid* at 8.
72 *Ibid* at 10.
73 *Ibid* at 11.
74 *Ibid* at 12.
75 *Ibid* at 16.
76 *Ibid* at 14–17.
77 *Community Safety and Correctional Services*, *supra* note 8 at paras 22–23.

(3) whether the Commissioner erred by interpreting the scope of *FOIPP* (ON)'s law enforcement exceptions by applying an elevated evidentiary standard to those provisions.[78]

The issue of whether the information requested by the journalist constituted personal information under *FOIPP* (ON) was not directly before the Supreme Court. Nevertheless, the question of whether the number of sex offenders per FSA constituted personal information underscored the Court's reasons in relation to the third issue on appeal. This was because the Court, in considering the evidentiary standard for the law enforcement exemptions, agreed with the adjudicator's view that the risks addressed by both exceptions were dependent on the risk of identification of one or more individuals. In this regard, the decision represents the Supreme Court's endorsement of what is needed to establish what information is personal information under section 2(1) of *FOIPP* (ON), and respectively what is needed to establish identifiability as described in *Pascoe*.[79]

The Court held that the standard of review was one of reasonableness and dismissed the appeal, finding in favour of the Commissioner on the remaining two questions.[80] The Court looked to the evidence provided by the Ministry in support of its claims. The Court noted that the Ministry had provided newspaper articles reporting past violent events, including murder and harassment of offenders whose location was publicly known.[81] These were characterized as unconvincing since they related to situations where offenders were already specifically identified in publicly available registries.[82] The Court was unconvinced by the Ministry's references to cases of identification facilitated by "detailed personal information in online registries available in other jurisdictions," presumably because the Court did not see a sufficient relationship between that information and the less specific FSA information at the centre of the appeal.[83] The Court appears to suggest that, for this additional registry

---

78 *Ibid* at para 24.

79 The Ministry argued that the adjudicator had taken too narrow a view of the law enforcement exemptions and that the risks addressed by these exemptions remained relevant even where no person is identified. As such, the Ministry argued that the OIPC had wrongly restricted the focus to the risk of identification of sex offenders. The Ministry explained that "[c]ommunity unease and vigilantism can arise from concern about the presence in the neighbourhood of any registered sex offender regardless of his identity" (Factum of the Appellant, *supra* note 64 at para 44) and that a sex offender who knows of his community's concern about his presence may, even without having been identified directly, move without reporting the change to the OSOR (*ibid*). The Court rejected this argument, however, finding that the Ministry had not provided sufficient evidence to illustrate the risk without identification (*Community Safety and Correctional Services*, *supra* note 8 at paras 39–40).

80 In its response to the final question, where the issue of personal information and the threshold for identifiability as defined in *Pascoe* were revisited, the Court reviewed the standard of proof set by the Commissioner with regards to the law enforcement exemptions claimed by the Ministry and determined that no reviewable error had been made on that point. The standard of proof set out by the Commissioner was, for the endangerment of life exemption under *FOIPP* (ON) section 14(1)(e), a "reasonable basis for believing" that the harm would occur, and for the exemption protecting the control of crime under section 14(1)(l), a "reasonable expectation of harm" supported by "detailed and convincing evidence." The standard for each exemption was specifically distinguished from a "speculation of possible harm," which the Court agreed would not suffice to justify the application of either law enforcement exemption: *Community Safety and Correctional Services*, *ibid* at paras 59, 65.

81 *Ibid* at para 60.

82 *Ibid*. See also Factum of the Appellant, *supra* note 64 at paras 27, 34.

83 *Community Safety and Correctional Services*, *ibid* at para 60. The arguments appear to have been made in relation to publicly available American registries, which provide detailed information about sex offenders, and specifically the high profile case of the Nova Scotia man who murdered two sex offenders in Maine after accessing their personal information on the State's publicly available registry of sex offenders: see "Maine Murders Baffle Police," *supra* note 35; Factum of the Appellant, *supra* note 64 at para 9. As an example of what can be found on the open registries in the US, Maine's sex offender registry currently allows the public to access information relating to a sex offender's name, known

information to have been relevant to the re-identification issue, the Ministry would have had to show a sufficient connection between the information available in public registries that was presented as evidence, and the FSA information sought by the journalist in this particular case.[84] The Ministry also presented what the Court characterized as "unconvincing and generic scholarly research" relating to identifiability, which did not address the specific facts in the case at hand.[85] Finally, the Court noted that the Ministry had "referred vaguely to the unpredictability of internet developments" without specifically showing how re-identification of the information under consideration could result from cross-referencing or other uses of publicly available information.[86] Having reviewed the Ministry's arguments and finding each insufficient to show a reasonable expectation of identification based on the FSA information, the Court upheld the Commissioner's decision on this point as reasonable.[87]

The outcome in *Community Safety and Correctional Services* can partly be attributed to the Ministry's failure to discharge its burden of showing that the information should be subject to one of the exemptions within the access to information scheme. At the same time, the courts are requiring evidence that may be difficult to obtain. Though the Court did not specify the type of evidence that would have sufficed to discharge the evidentiary burden attached to the *Pascoe* standard for identifiability, the decision allows for some general conclusions based on what was insufficient to convince the judges of a reasonable expectation of identification in the circumstances. By rejecting stories of identifications and "generic scholarly research," the Court suggested that evidence in future cases will need to be directly linked to the specific data set at issue before the courts will be convinced of a reasonable expectation of identifiability. By deciding in favour of disclosure where the risk cannot be proven, the Supreme Court of Canada clearly tried to avoid a situation where information is withheld based on speculative risk. Finally, by rejecting arguments about expected advancements in Internet and information technologies, the Court indicated that the standard will, in the future, be judged according to the information technologies in existence when each case is heard.

In this light, it is easy to see why the Court's decision was heralded as a victory for transparency. It leans heavily towards the disclosure of information that does not directly identify individuals, so long as identifiability cannot clearly be established. However, the Court's approach may short-change privacy considerations. In our current information environment, the amount and nature of available information changes rapidly, with the

---

aliases, physical description, date of birth, photograph, mailing and home address or place of residence, place of employment, place of school attendance, and details relating to the crime that led to registration: Maine, Department of Public Safety, "Maine Sex Offender Registry," online: <sor.informe.org>.

84 Note that in *Ontario (AG) v Pascoe* (2001), 154 OAC 97 at para 20 (Sup Ct J), there was also an issue of the relevant Ministry's failure to meet the necessary evidential burden. The Court found the adjudicator's conclusion on this point to be reasonable.

85 *Community Safety and Correctional Services*, *supra* note 8 at para 60. Academic literature on re-identification risk explores the extent to which apparently anonymized data can be linked to specific identifiable individuals: see e.g. Ohm, *supra* note 22; Latanya Sweeney, "*k*-Anonymity: A Model for Protecting Privacy" (2002) 10:5 Intl J Uncertainty, Fuzziness & Knowledge-Based Systems 557; Khaled El Emam, Ann Brown& Philip AbdelMalik, "Evaluating Predictors of Geographic Area Population Size Cut-offs to Manage Re-identification Risk" (2009) 16:2 J American Medical Informatics Assoc 256. It is important to note that the Supreme Court of Canada in *Community Safety and Correctional Services* is not dismissing the validity of this literature — rather, it is declining to find, in the abstract, that there is a re-identification risk without some evidence related to the particular data at issue.

86 *Community Safety and Correctional Services*, *ibid* at para 61.

87 *Ibid*.

sources of data being multiple and diffuse.[88] Not only is there more and more data being made available on a daily if not hourly basis, but more and more data is also being collected by multiple actors.[89] A 2014 report indicated that the digital universe is growing by 40 percent each year.[90] Rob Kitchin and Tracey Lauriault attribute this increase to the "continuous and exhaustive" production of data, noting that the private sector, including social media companies, harvest masses of data on an ongoing basis.[91] Meanwhile, information technologies will surely continue to advance, which may enable identification of individuals through use of information currently being released within today's access to information (or open data) framework, in addition to information from other sources.[92] This multiplicity of sources and new analytical techniques present a further challenge. Although it would still be immensely difficult to identify all publicly available data sets that might be useful in a re-identification exercise, the reality is that not all data sets are publicly available.[93] Data released by government may be matched with compilations of data in private hands for a broad range of profiling and analytic purposes.[94] A high threshold for establishing a re-identification risk opens up government data to this type of analysis and poses a risk to privacy. Ohm illustrates the problem by recounting the failures of anonymization techniques, which were for many years touted as the answer to striking a balance between individual privacy interests and public access to information.[95] In contrast to the Court's position that risks must be determined based on the evidence relating to identifiability as it exists today, Ohm advocates an "aggressively pessimistic assumption of

---

88 Kitchin & Lauriault, *supra* note 2; Kitchin, *Data Revolution*, *supra* note 1 at 67–79.

89 Recent estimates indicate that approximately 90 percent of the world's data has been created in the last two years: see Jodi LeBlanc, "Understanding Open Data: Don't get left behind" (18 February 2014), *Canadian Government Executive* (blog), online: <cgexecblog.wordpress.com/2014/02/18/understanding-open-data-dont-get-left-behind>. Discussing the changes in data collection practices by both the public and private sector in the knowledge-economy and information age, Cynthia Gayton notes that "[l]ittle by little, seemingly insignificant pieces of data are being collected by not only the government entities and companies with whom consumers conduct business, but third party data brokers" (Cynthia M Gayton, "Beyond terrorism: data collection and responsibility for privacy" (2006) 36:4 J Information & Knowledge Management Systems 377 at 377). See also Jane Bailey, "Systematic government access to private-sector data in Canada" (2012) 2:4 Intl Data Privacy L 207 (noting that Canada's *Privacy Act* and *Personal Information and Protection of Electronic Documents Act* both include numerous exceptions that allow information sharing among government entities and between the public and private sector); Kitchin & Lauriault, *ibid*. Big data cities are also harnessing more and more information, for instance as part of the "smart city" initiatives seen across Canada: see e.g. Liz Enbysk, "Vancouver, B.C. proposes $30M smart cities plan," *Smart Cities Council* (18 April 2013), online: <smartcities council.com/article/vancouver-bc-proposes-30m-smart-cities-plan>; IBM, "Waterfront Toronto Teams with IBM to Build a Smarter City," *IBM News* (18 September 2013), online: <www.ibm.com/news/ca/en/2013/09/18/d784454e42662t01.html>; The Smart Cities Daily, "Smart City Expo Montreal" (2014), online: <www.smartcityexpomtl.com/ca/blog>.

90 EMC, "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things" (2014), online: <www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm>.

91 Kitchin & Lauriault, *supra* note 2. See also LeBlanc, *supra* note 89.

92 Kitchin & Lauriault, *ibid*; Kitchin, *Data Revolution*, *supra* note 1 at 166.

93 Data brokers' files, for example, are not publicly available, and are generally maintained under strict conditions of secrecy. US, Senate Committee on Commerce, Science and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (Washington, DC: 18 December 2013) at 12–13, online: <www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577 [Committee on Commerce].

94 The Committee on Commerce, Science and Transportation, in its recent report, identified "government records and other public data" as a primary source of data for big data brokers (*ibid* at 15). On private citizen access and use of open government data, see Kitchin, *Data Revolution*, *supra* note 1 at 62-66.

95 Ohm, *supra* note 22 (notes that privacy lawyers may also refer to "release-and-forget anonymization techniques" as "deidentification" or the "removal of personally identifiable information" at 1716) See also Khaled El Emam, Elizabeth Jonker & Anita Fineberg, *The Case for De-Identifying Personal Health Information* (Ottawa: CHEO Research Institute, 2011) (definition of "de-identification" more specifically as "a set of methods that can be applied to data to ensure that the probability of assigning a correct identity to a record in the data is very low" at 6).

perfect outside information" that may facilitate future re-identifications following disclosure of useful data sets that have purportedly been de-identified.[96] He predicts that re-identification risk will continue to rise along with advances in computer software and availability of outside information, and that "computer scientists and talented amateurs" will continue to re-identify individuals through data sets released under the assumption of anonymity. Further, Ohm predicts that these re-identifications will be done cheaply, quickly, and easily.[97] Based on this projection, he rejects the idea that certain kinds of information can be singled out today as less likely to lead to re-identification.[98]

Ontario's former Privacy Commissioner clearly disagrees with the message put forth by Ohm and others. She suggests that the risk of re-identifying de-identified data has been exaggerated and, while admitting that previous de-identification techniques have fallen short as evidenced by re-identifications in specific circumstances, argues that the right way forward is to rely on more rigorous standards for de-identification.[99] Others appear to be more convinced of the risks. In light of recent concerns about the weaknesses of the anonymization and the risks of re-identification, United States policymakers have been refining their requirements on data sets that can be released, including a specific requirement that postal codes released in data sets relating to health information must be limited to two digits for areas with 20,000 or fewer residents.[100] Moreover, it is conceivable that the risk of re-identification that Ohm warns against is already being realized, as re-identification may be accomplished through the use of privately owned or less-publicly accessible information.[101] If this is so, the problem for cases like *Community Safety and Correctional Services* is clear: without access to the additional information that may facilitate these types of re-identifications, it is not possible to show the risk ahead of time and is therefore not possible to meet the burden of proof expected by the courts.

*Community Safety and Correctional Services* is a case that arose in the access to information context. As a result, it was a specific request for the disclosure of certain data that was under the microscope. The challenge is to translate this context to one in which proactive disclosure and open data are to become routine. It is important to consider what processes will be put in place to ensure that the information disclosed strikes an appropriate balance between privacy and transparency. Rather than having specialized tribunals adjudicate disclosure issues, both proactive disclosure and open data call upon bureaucrats

---

96 Ohm, *ibid* at 1725.

97 *Ibid* at 1731.

98 *Ibid* at 1732.

99 Ontario, Information and Privacy Commissioner, "Big Data and Innovation, Setting the Record Straight: De-Identification *Does* Work" by Ann Cavoukian & Daniel Castro (Toronto: OIPC, 16 June 2014), online: <www.ipc.on.ca/images/Resources/pbd-de-identification_ITIF.pdf>; Ontario, Information and Privacy Commissioner, "Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy" by Ann Cavoukian & Khaled El Emam (Toronto: OIPC, June 2011), online: <www.ipc.on.ca/images/Resources/anonymization.pdf>. See also Khaled El Emam et al, "A Globally Optimal k-Anonymity Method for the De-Identification of Health Data" (2009) 16:5 J American Medical Informatics Assoc 670; Khaled El Emam, "Methods for the de-identification of electronic health records for genomic research" (2011) 3:4 Genome Medicine 25 (discussing de-identification standards, re-identification risk, and the need for research into improving methods for the de-identification of genomic data; El Emam, Jonker & Fineberg, *supra* note 95 (outlining scenarios in which de-identification can be of value to data custodians).

100 See *Health Insurance Portability and Accountability Act*, 45 CFR § 164.514(b)(2)(B) (2009), cited in Ohm, *supra* note 22 at 1737, n 184.

101 Ohm, *ibid* at 1729.

to make these decisions — and to make them in a context where there are limited resources and quite possibly no formal training. If it is impossible to know whether information is personal information without considering the other available information with which it might be matched, how are such considerations to be taken into account? What types of privacy harms are we prepared to risk in the interests of transparency?

In *Community Safety and Correctional Services*, the Supreme Court appears to indicate that, in circumstances like those presented in the case, evidence being introduced to support an exception to disclosure based on a risk of identifiability must have a sufficient relationship with the information at issue to be considered relevant. The developing scholarship in the area will only be considered relevant to the extent that it specifically addresses a risk of re-identification for the circumstances and type of information at issue. The Court appears to set a threshold that requires evidence that may be very difficult for the government to obtain. By deciding in favour of disclosure when this threshold for showing re-identification risk cannot be met, the Court arguably gives insufficient weight to the long-term privacy considerations that are relevant in the access to information, open data, and proactive disclosure contexts. These privacy risks are amplified by several factors that will become increasingly important over time, specifically that: (1) more and more data is being collected by both public and private sector actors; (2) the full nature and amount of data that is currently held by private sector actors is unknown; (3) an increasing amount of data is becoming available in the online world; (4) information technologies that will assist in re-identifying individuals are continuously advancing while also becoming more accessible and affordable; and (5) anonymization techniques are proving to be less reliable than previously believed. Finally, given the complexity of the privacy issues that underlie the circumstances of *Community Safety and Correctional Services* and that were not fully explored within the judgment, there is a valid concern about the extent to which this judgment will inform decisions made by those responsible for releasing government-held information in the developing open data and proactive disclosure environments. This is particularly the case given that many of these individuals do not possess the resources or training to assess the re-identification risk inherent in each new data set. With these issues in mind, the next section of this article considers the other side of the balance, and asks whether the disclosure of the requested information in *Community Safety and Correctional Services* genuinely served the objectives of transparency.

## IV. DEFINING TRANSPARENCY IN THE DEVELOPING BIG DATA ENVIRONMENT

The right of access established by access to information legislation in Canada is not explicit about transparency as an underlying value, nor is accountability in general explicitly mentioned in the legislation. Nevertheless, access to information regimes are widely understood to promote both transparency and accountability of governments.[102] The

[102] The statement of purpose in the federal *Access to Information Act*, *supra* note 49, s 2, emphasizes the need to provide the public with a right of access to government records "in accordance with the principles that government information should be available to the public." "Canada's Action Plan," *supra* note 6, outlines existing legislation that aims to promote transparency and openness in government, including access to information laws. The National Research Council discusses how compliance with access to information and privacy legislation represents its commitment to transparency: see National Research Council Canada, "Access to Information and Privacy Acts (ATIP),"

importance of access to government information is reflected in the growing recognition of the right of access at the international level.[103] In the case of access to information, transparency is given a particular context — typically there is a request by an individual or an organization that seeks access to certain information for particular purposes. In the context of open data or proactive disclosure of government information, the link to transparency is more oblique. While information that tends to be highly sought-after under access to information regimes may be high on the list for proactive disclosure, and while information may be ranked as high value or low value according to some concept of transparency,[104] proactive disclosure and open data occur as a result of particular requests for information, and it may be necessary to give particular attention to the transparency value of the disclosed information if a potential privacy risk exists.

Transparency is linked to government accountability, and both concepts relate to the public's ability to address deficiencies in government and to support democratic values.[105] History has shown that traditional methods of ensuring political accountability, such as regular elections or government audits, do not provide sufficient protection against corruption.[106] Accordingly, by facilitating a more informed and engaged public, open data and proactive disclosure may fill the gap in ensuring accountability for public institutions.

Although it is clear that greater transparency in government operations is desirable, the concept of transparency itself has not been consistently defined.[107] Some views of transparency appear to require that the government release as much information to the public as possible. This is reflected in open by default approaches, which appear in a number of the emerging open government policy documents.[108] The idea in this view of transparency is that

---

online: <www.nrc-cnrc.gc.ca/eng/transparency/access_information/index.html>. Finally, the relationship between access to information laws and transparency and accountability in government has been discussed by Canadian courts, including for instance *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, 2010 SCC 23, [2010] 1 SCR 815 at para 1 [*Criminal Lawyers' Association*]; *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25, [2011] 2 SCR 306 at para 80; *Nault v Canada (Public Works and Government Services)*, 2011 FCA 263, [2013] 2 FCR 491 at para 27.

103 Janssen, "Open Government," *supra* note 5.

104 The Canadian government has identified four high priority categories of information: national statistics, election results, government budget information, and national maps. Secondary areas of "high value data" relate to companies, crime and justice, earth observation, education, energy and environment, finance and contracts, geospatial data, global development, government accountability and democracy, health, science and research, social mobility and welfare, statistics, and transportation and infrastructure: "G8 Open Data," *supra* note 7. Priority goals are also emerging in other jurisdictions, for instance in the Obama administration's policy which is recognized as primarily serving goals of increased transparency, public engagement, and collaboration. Also, the European Commission emphasizes economic gains to be derived from the open data movement (Zuiderwijk & Janssen, *supra* note 41 at 17). The need for further research to identify priority goals is emphasized in Janssen, Charalabidis & Zuiderwijk, *supra* note 41 at 266; Zuiderwijk & Janssen, *supra* note 41 at 25. The Canadian government has committed to engaging with the public to assess user needs and interests, including through public consultations, round table discussions, and surveys ("G8 Open Data," *supra* note 7).

105 John Gaventa & Rosemary McGee, "The Impact of Transparency and Accountability Initiatives" (2013) 31 Development Policy Rev s3 at s4.

106 *Ibid*.

107 See *ibid* (where the authors emphasize the need to understand the meaning of accountability and transparency, noting that the increasingly common "'social', 'citizen-led' or 'demand side'" accountability initiatives regularly invoke these values "to the point where 'accountability' and 'transparency' are at risk of becoming buzzwords" at s4 [citations omitted]).

108 See e.g. House of Commons, Standing Committee on Government Operations and Estimates, *Open Data: The Way of the Future* (June 2014) (Chair: Pierre-Luc Dusseault) at 5 [Committee on Government Operations]; "G8 Open Data," *supra* note 7; Ontario, Open Government Engagement Team, "Open by Default: A new way forward for Ontario" (Toronto: Queen's Printer, March 2014), online: <https://dr6j45jk9xcmk.cloudfront.net/documents/2428/open-by-default-2.pdf> ["Open by Default"

government decision-makers will ensure the legality of their decisions due to the potential exposure of their actions.[109] Other definitions of transparency focus on the potential for the public to use the information that is provided. This view defines transparency as the act of making relevant, timely, and useful information available to the public in easy-to-access formats.[110] More abstract conceptions of transparency focus on the ways in which the release of government-held data leads to a more informed public. For instance, one definition of transparency is the "degree to which the existence, content, or meaning of a law, regulation, action, process, or condition is ascertainable or understandable by a party with reason to be interested in that law, regulation, action, process, or condition."[111] Elsewhere, transparency has been said to have a variable meaning that is connected to its purpose, which may sometimes be to simply make information available, but may at other times be to encourage participation, or to facilitate accountability for a government or other type of organization.[112] In *Community Safety and Correctional Services*, both the Ministry and the Commissioner characterized the overarching purpose of the access to information framework as the encouragement of democratic participation, a goal that is intricately tied to government accountability.[113] The Court has elsewhere emphasized that the value derived from the access to information scheme relates to all three of the above purposes.[114]

While both the Supreme Court of Canada and the Information and Privacy Commissioner of Ontario linked the *Community Safety and Correctional Services* decision to the value of transparency, there is little analysis of how transparency is actually served in this instance.[115]

---

ON]; Alberta, "Government of Alberta Open Information and Open Data Policy," online: <data.alberta.ca/content/government-alberta-open-information-and-open-data-policy> ["Open Data Policy," AB].

109 See Carsten Grønbech-Jensen, "The Scandinavian tradition of open government and the European Union: problems of compatibility?" (1998) 5:1 J European Public Policy 185 (where the author discusses the different notions of transparency within Sweden and Denmark but notes that both jurisdictions relate the concept of transparency to the public's right of access in order to ensure legitimacy of the decision-makers and public actors and to "maintai[n] the status of the citizen as the central locus of attention in public policy" at 188).

110 Health Canada, "Regulatory Transparency and Openness," online: <www.hc-sc.gc.ca/home-accueil/rto-tor/index-eng.php>.

111 William Mock, "On the Centrality of Information Law: A Rational Choice Discussion of Information Law and Transparency" (1999) 17:4 John Marshall J Computer & Info L 1069 at 1082 [emphasis omitted].

112 Jason Potts, Jessica van der Meer & Jaclyn Daitchman, *The State of Sustainability Initiatives Review 2010: Sustainability and Transparency* (Winnipeg: International Institute for Sustainable Development and the International Institute for Environment and Development, 2010) at 125.

113 See comments in *Community Safety and Correctional Services*, *supra* note 8 (Factum of the Respondent at para 86) [Factum of the Respondent]; Factum of the Appellant, *supra* note 64; *Dagg*, *supra* note 55 at para 61, which was relied upon by both the Ministry and the OIPC in Factums to the Supreme Court. See also Ontario, Information and Privacy Commissioner, "Access by Design: The 7 Fundamental Principles" by Ann Cavoukian (Toronto, OIPC, April 2010), online: <www.ipc.on.ca/images/Resources/accessbydesign_7fundamentalprinciples.pdf>.

114 See *Criminal Lawyers' Association, supra* note 102, McLachlin CJC and Abella JA (noting where the Supreme Court noted that "[a]ccess to information in the hands of public institutions can increase transparency in government, contribute to an informed public, and enhance an open and democratic society" at para 1).

115 Christopher Berzins has noted a complex issue is at play in terms of the OIPC's role in access information disputes at the tribunal level and later as an interested party in judicial review of those decisions. He notes that the courts have expressed concerns over tribunal involvement in aggressive defence of their decisions, as this might impair their impartiality in the tribunal process. The OIPC, however, serves a mandate that includes advocating for the types of issues that arise in access to information disputes. The issue is linked to the quality of reasoning in tribunal decisions, as the courts might be skeptical of arguments advanced on behalf of the Commissioner if these were not explored within the tribunal decision itself: see Berzins, *supra* note 39 at 95. Viewed against the lack of analysis of the concept of transparency in *Community Safety and Correctional Services*, it is worth considering whether the conflicting roles played by the OIPC might have played into the reserved judgment, which did not engage in a full analysis of the important concept of transparency as it relates to the value of

Whether greater transparency was actually achieved in the case depends on the definition of transparency upon which a potential analysis of the issue relies. To the extent that transparency is viewed as requiring only that information be made available to the public unless a valid exception can be shown to apply, the decision can be viewed as having promoted the value of transparency. If, however, transparency is linked to the aim of supporting a more informed and engaged public, the merits of this decision become less clear.

In assessing whether the decision represents a win for transparency, it is also important to point out that the information in this case was not about the operation of government. Rather, it was location information regarding sex offenders who had registered under a provincial system implemented by a law in which the explicit policy choice made was to not disclose the location of registered sex offenders. This lack of public access to this information was specifically debated and approved by the legislature. In *Community Safety and Correctional Services*, the Ministry tried unsuccessfully to convince the Supreme Court that the information about the OSOR that had already been released by the Ministry (general statistical information about the number of sex offenders registered on the OSOR, data relating to the frequency with which the police access the registry, and a detailed report released by the Auditor General reviewing the effectiveness of the registry) served to ensure transparency and supported an informed public when it comes to OSOR operations.[116] The rejection of this argument suggests that, despite the policy decision to withhold the information, the Court found that the statistics and formal report gave insufficient details on OSOR operations, or alternatively accepted that more information is better when it comes to public knowledge about government operations.

A second issue is that the public's ability to become more informed about government operations depends on the quality and accuracy of the information it receives. This point applies whether the data becomes available through broad dissemination by an individual who obtained the information in the access to information context or through open data or proactive disclosure initiatives. Before examining issues regarding data quality, it is important to emphasize that the discussion is not provided as an argument for more limited release of government data in the access to information, open data, or proactive disclosure contexts. Rather, it is used to highlight issues that have been well-explored in the data sciences context: issues of data quality, fitness for purpose, and metadata.[117]

---

privacy. See also Gaventa & McGee, *supra* note 105 at s12, where the authors note that, "many initiatives are not underpinned by a clear articulation of exactly what outcome or impact is sought, or of how the actions and inputs contemplated are expected to generate that outcome or impact." They further note at s16 that the lack of research outlining a clear understanding of the expected outcome of transparency and accountability initiatives is evident even with respect to access to information schemes, which have been operating for much longer than open data and open government. They suggest that, with respect to access to information regimes, this may be in part because of the prevalent view of access to information rights as rights in themselves.

116 Factum of the Appellant, *supra* note 64 at para 52. For the Auditor General's review of the OSOR, see Office of the Auditor General of Ontario, *2007 Annual Report* (Toronto: Queen's Printer, 2007) at 19–20 [*AG's Annual Report, 2007*]; and a progress update in Office of the Auditor General of Ontario, *2009 Annual Report*, (Toronto: Queen's Printer, 2009) at 414–19 [*AG's Annual Report, 2009*].

117 Metadata is used here to mean, in its simplest sense, "data about the data." Metadata more broadly is information that can identify the contents of any data sets as well as its limitations.

It is arguable that government transparency and the public's ability to enforce accountability are best facilitated where the public is given access to information that is accurate. The Canadian government has acknowledged this need for accurate information as part of its efforts to provide its citizens with the information needed to hold the government accountable in relation to its use of public funds.[118] In its "Federal Accountability Action Plan," the then-newly elected Conservative government stated that:

> Improving the transparency and credibility of the Government's fiscal forecasting and budget planning process is a fundamental step in making it more accountable to Parliament and to Canadians. Parliamentary committees should have access to independent, objective analysis and advice on economic and fiscal issues, supported by the timely provision of accurate information from departments and agencies.[119]

Similarly, in the employment equity context, the government has acknowledged the need for access to the most accurate and up-to-date information on the workforce in order to allow organizations like the Public Service Commission and Canadian Human Rights Commission to hold the government accountable for its promises and programs concerning workplace issues.[120]

If inaccurate information about government operations is disseminated to the public, it may not contribute to greater transparency within government. Transparency could still potentially be facilitated by a resulting debate over the information itself, though this represents a different benefit than that envisioned by the above definitions in which the focus is largely on greater public knowledge of government activities, spending, and general decision-making. Yet, extolling the decision in *Community Safety and Correctional Services* without acknowledging the limitations of the information ordered for release may deflect from some important considerations that should play a role in the general response to the decision.

Considering the accuracy and quality of the information received by the public through the OSOR map, it is clear that there are a number of ways in which it might mislead and even harm the public. To complement its release of the map, Global News drew a number of conclusions based on the data, including that:

- Since 2008, sex offender rates have risen in certain areas of Ottawa and Hamilton;
- Since 2008, sex offender rates have dropped in certain "gentrifying neighbourhoods" in Toronto;

---

118 Note that while the word "citizens" is used in this publication and other government documents discussing transparency and access to information issues in Canada in the more restrictive sense relating to immigration and citizenship, the issues as they are discussed in this paper are meant to include any stakeholders with an interest in government activities, such as Canadian citizens, residents, other government departments, and other users of information disclosed by government.

119 Treasury Board of Canada Secretariat, "Canada's New Government: Federal Accountability Action Plan: Turning a New Leaf" (Ottawa: TBCS, 11 April 2006) at 13, online: <www.tbs-sct.gc.ca/fac-lti/docs/ap-pa/ap-pa-eng.pdf>.

120 Senate, Standing Senate Committee on Human Rights, *Reflecting the Changing Face of Canada: Employment Equity in the Federal Public Service* (June 2010) (Chair: Janis G Johnson) at 60. See also Mock, *supra* note 111 at 1081.

- That there are "clusters" of sex offenders in certain parts of Kingston, London, and Peterborough;
- That sex offenders often settle in low-income neighbourhoods.[121]

Both the map itself and the conclusions drawn from the representation of the data may, at first, appear useful in terms of public knowledge about the whereabouts of sexual offenders in Ontario. In terms of enforcing government accountability, such information might lead concerned citizens, residents, and other interested parties to demand that resources be devoted to high risk areas as depicted on the map, or it might be used as evidence that police did not devote proper attention to high risk areas following a sexual assault in a given area. The map might also be used by the public to determine the relative safety of a given area, which would perhaps be of interest to those contemplating a move to or within Ontario, or those trying to determine what precautions are needed in the neighbourhood in which they already reside. The adjudicator in *Community Safety* OIPC clearly accepted this logic, arguing that the FSA maps could "promote public safety by making people aware that, in those areas, their risk of being subject to an attack may be higher."[122] A closer look at the information as it is presented, however, reveals a number of ways in which the public might be misled by the visual representation of the OSOR information and the sweeping conclusions drawn by the media as the map was disseminated. It is arguable that the overall effect of the release of this information is neither greater transparency in terms of government operations, nor a more informed public in terms of risks to personal safety.

For starters, the information cannot tell the full story of the whereabouts of sex offenders in Ontario.[123] For a number of reasons, it should not be assumed that all sex offenders living in Ontario have been included on the registry, or correspondingly on the map compiled from the OSOR information. The registry does not, for instance, include up-to-date information on offenders who, following disclosure of the information, were released into the community after completion of the custodial portion of their sentences (with or without complying with the requirement to report to police).[124] The map does not reflect the whereabouts of offenders who have recently moved (again, with or without complying with the requirement to notify police). As the OSOR scheme applies only to adult offenders and to young offenders tried or sentenced as adults, the map does not include any young offenders who have committed

---

121 Cain, "Sex Offender Map," *supra* note 34. The website includes a link to the raw data along with an invitation to others to work with it. It superimposes the map onto previously compiled maps to show correlations between sex offender whereabouts and an area's violent crime rates as well as family income. The website argues that transparency is served simply by having more access to more information. It only briefly discusses, then dismisses, the privacy risks attached to greater transparency and access to information. In terms of qualifying the data as presented, the narrative explanation provided with the map gives limited information about the content and limitations of the data. Much of this information is provided in text that appears well below the map, and follows a lengthy discussion of the court battle as well as details on what the map purportedly reveals.

122 *Supra* note 26 at 15. See also Factum of the Respondent, *supra* note 113 at para 11.

123 Note that the data refers only to registered sex offenders (as is discussed below). However, the narrative explanation and analysis provided with the map uses, in an apparently interchangeable way, "registered sex offenders" and "sex offenders." This may contribute to uncertainty among some users as to what exactly is revealed by the data: see Cain, "Sex Offender Map," *supra* note 34.

124 *AG's Annual Report 2007*, *supra* note 116 at 19–20; *AG's Annual Report, 2009*, *supra* note 116 at 414–19.

sexual offences but do not fall into the latter category.[125] Furthermore, the map may be missing information on certain offenders who served their sentences under federal custody.[126]

There are several other reasons to question the accuracy of the map. The map does not include the temporary location of sex offenders who have been granted unsupervised passes from correctional facilities.[127] Moreover, offenders report to the OSOR for different time periods that depend on the relative severity of the offence committed. While those convicted of more than one sexual offence or of offences for which the maximum sentence is more than ten years must report for life, individuals convicted of sexual crimes for which the maximum sentence is less than ten years are generally required to report to the OSOR for a defined period of ten years, which may end sooner if a pardon is granted.[128] The map therefore does not include information on the whereabouts of convicted sex offenders in the latter category who have fulfilled their personal reporting requirements, nor does it include sex offenders who have been pardoned.[129]

In addition, the nature and reality of the criminal process relating to sex offences undoubtedly affects the accuracy of the map. The map does not reflect the unknown number of individuals who were not charged, those who were acquitted of charges for a sexual offence but were in fact guilty, or those who were initially charged with offences of a sexual nature but who entered into a plea bargain leading to a conviction for a non-sexual offence.[130] Finally, because sex offences remain one of the most severely under-reported crimes in Canada, many sex offenders undoubtedly live freely within our communities.[131]

---

125 *Christopher's Law*, *supra* note 27, s 8(2).

126 *AG's Annual Report 2007*, *supra* note 116 at 19; *AG's Annual Report, 2009*, *supra* note 116 at 414.

127 Note, however, that the correctional facility from which an offender is released on a temporary pass must notify the Ministry of Community Safety and Correctional Services (*Christopher's Law*, *supra* note 27, s 4.1). Many of the issues pertaining to the accuracy of the OSOR information were brought up as part of a review of the OSOR operations, conducted by the Office of the Auditor General of Ontario in 2007. The Ministry of Community Safety and Correctional Services, along with police services and other interested and involved parties, have been working to address some of the problems identified by the review, though it is recognized that the process of improving the OSOR will be long-term, so the issues still play into the accuracy and completeness of the registry today. See *AG's Annual Report, 2007*, *ibid* at 19–20; *AG's Annual Report, 2009*, *ibid* at 414–19.

128 *Christopher's Law*, *ibid*, s 7.

129 This particular limitation was alluded to in the article accompanying the release of the map. Without going into detail about how this factor limits the accuracy of the map, Cain states: "Ontario's registry requires people convicted of various sexual offences to register their home address with police for either 10 years or life. Offenders who are pardoned can be taken off the registry. They don't register while in prison" (Cain, "Sex Offender Map," *supra* note 34).

130 The difficulties in proving charges relating to sexual assaults are particularly acute, due in part to the fact that the Crown's case most often relies primarily on the victim's testimony and the difficulty of proving that the sexual activity occurred without the victim's consent: see Alberta, Justice and Solicitor General, *Best Practices For Investigating and Prosecuting Sexual Assault* (Edmonton: Justice and Solicitor General Criminal Division, 2013) at 8, online: <www.justice.alberta.ca/programs_services/criminal_pros/Documents/SexualAssaultHandbook-PoliceCrown.pdf> [*Best Practices*]. In a recent study of criminal court statistics in Canadian adult courts, it was noted that the extent to which plea-bargaining is used in Canada is unknown: see Statistics Canada, "Adult criminal court statistics in Canada, 2010/2011" by Mia Dauvergne, in *Juristat*, Catalogue No 85-002-X (Ottawa: Statistics Canada, 28 May 2012), online: <www.statcan.gc.ca/pub/85-002-x/2012001/article/11646-eng.pdf>. Recent statistics about the overall rates of sexual offenders that are held accountable indicate that as few as 0.3 percent are convicted of their crimes: see Holly Johnson, "Limits of a Criminal Justice Response: Trends in Police and Court Processing of Sexual Assault" in Elizabeth A Sheehy, ed, *Sexual Assault in Canada: Law, Legal Practice and Women's Activism* (Ottawa: University of Ottawa Press, 2012) 613 at 632.

131 Ontario, Ontario Women's Directorate, "Statistics: Sexual Violence" (Toronto: OWD, 2009) at 2 [Ontario Women's Directorate]. It is estimated that less than 10 percent of sexual assaults are actually reported to Canadian police: see Statistics Canada, "Police-reported crime statistics in Canada, 2011," by Shannon Brennan, in *Juristat*, Catalogue No 85-002-X (Ottawa: Statistics Canada, 24 July 2012), online: <www.statcan.gc.ca/pub/85-002-x/2012001/article/11692-eng.pdf>; *Best Practices*, *ibid* at 5.

To the extent that the public may use the map to judge the level of safety or need for law enforcement resources in a given community, there are additional issues to consider in terms of the information that the map conveys. The OSOR scheme includes offenders convicted of crimes ranging from exposure to invitation to sexual touching to sexual assault with a weapon, though the map does not indicate the severity of the offences committed by the offenders that it aims to represent.[132] If the map is used to determine possible threats to safety, information relating to the previous offences committed by a potential perpetrator, such as whether physical force was used during the commission of the crime or whether a child or other specific type of victim was involved, would likely influence the precautions that might be taken to address the perceived threat to personal safety.[133] Though the Global News article accompanying the map notes that "stranger" attacks are rare compared to the number of sexual assaults committed by perpetrators known to the victim, the idea that the public can use the map to increase personal safety may nevertheless reinforce the misconception that the public should be most concerned about the potential of being sexually assaulted by an unknown person.[134] Finally, by focusing the issue of community safety on the prevalence of sexual assault without providing any indication of the whereabouts of persons convicted of other crimes posing a threat to public safety, including, for instance, violent but non-sexual assaults, or armed thefts and burglaries, the map may distract from the reality that sex offences are only part of the criminal activity with which the public should be concerned.[135]

The above discussion reveals the importance of understanding the limitations of data in terms of fitness for purpose, as it is clear that a given data set may be well-suited for some analytical purposes but not fit for others due to the limitations of the data collected.[136] This underlines the importance of including metadata with information that is made available for secondary purposes. Secondary uses of data may separate information from its full record or original context, leaving data incomplete and vulnerable to misinterpretation.[137] It is the metadata that explains the parameters and limitations of the data set.[138] As seen in the example of the OSOR map, information that is provided without clear metadata can be highly

---

132 See the definition of "sex offence" for OSOR purposes in *Christopher's Law*, *supra* note 27, s 1.

133 This argument is backed up by research showing clear differences among sex offenders in terms of the risk for reoffence following treatment, victim profiles, and modus operandi. See generally Michael Woodworth et al, "High-risk sexual offenders: An examination of sexual fantasy, sexual paraphilia, psychopathy, and offence characteristics" (2013) 36:2 Intl J L & Psychiatry 144; Christine Janka et al, "The significance of offending behavior for predicting sexual recidivism among sex offenders of various age groups" (2012) 35:3 Intl J L & Psychiatry 159; Correctional Service Canada, "A Review of the Recidivism Rates of Adult Female Sexual Offenders," by Franca Cortoni & R Karl Hanson, Research Report No R-169 (Ottawa: CSC, May 2005), online: <publications.gc.ca/collections/collection-2010/scc-csc/PS83-3-169-eng.pdf>.

134 Strangers are the perpetrators in only 25 percent of sexual assaults: see Ontario Women's Directorate, *supra* note 131 at 3; *Best Practices*, *supra* note 130 at 17.

135 Cain alludes to this point by superimposing the sex offender map onto a map relating to violent crime (a threshold that is not defined). Moreover, the limitations of the violent crime map are not discussed at all: see Cain, "Sex Offender Map," *supra* note 34.

136 R Devillers et al, "Towards spatial data quality information analysis tools for experts assessing the fitness for use of spatial data" (2007) 21:3 Intl J Geographical Information Science 261; Sylvie Servigne, Nicolas Lesage & Thérèse Libourel, "Quality Components, Standards, and Metadata" in Rodolphe Devillers & Robert Jeansoulin, eds, *Fundamentals of Spatial Data Quality* (London: ISTE, 2006) 179; R Devillers et al, "How to Improve Geospatial Data Usability: From Metadata to Quality-Aware GIS Community" (Paper delivered at Spatial Data Usability AGILE Pre-Conference Workshop, Aalburg, Denmark, 8 May 2007), online: <www.mun.ca/geog/people/Faculty/rdevillers/Devillers_SDQ_Agile 2007.pdf>.

137 Yannoukakou & Araka, *supra* note 5 at 338.

138 Kitchin, *Data Revolution*, *supra* note 1 at 8–9.

misleading, and even harmful.[139] Marijn Janssen, Yannis Charalabidis, and Anneke Zuiderwijk have emphasized this risk, noting that:

> Opening data that has no adequate information quality can result in discussions, confusions, less transparency, and even in less trust in the government. The latter can be explained by the fact that resources are wasted and only fuzzy or even incorrect outcomes can be created when there is low information quality.[140]

The transparency value of released data can thus be considerably muted where the lack of sufficient metadata acts as a barrier to contextualization of the data.[141]

Another issue is that data is not neutral. This argument, which is advanced by critical data scholars, maintains that data is inevitably shaped by a host of decisions taken in relation to it that are not neutral or objective.[142] A decision by a government to conduct a demographic survey that asks some questions but not others results in a compilation of data that embeds the biases that shaped the framing of the questions. Data gathered using some media that are accessible only to certain segments of the population are similarly not neutral in that the responses are filtered through certain levels of privilege and access. The treatment of victims of sexual assault in the court system, with the result that conviction rates are low and the crime is grossly underreported, also skews data about the location of sex offenders. While concerns about the lack of neutrality of data are not reasons to argue against its release, they are reasons to argue for better metadata and heightened levels of data literacy among the general population and also among those who seek to use the data for journalism, research, or advocacy.

The need to incorporate metadata standards for information disclosed by the government has been raised in discussions around open data in Canada.[143] As of yet, there is no set standard for metadata across the different levels of government.[144] In contemplating the kind

---

139 Another example of the issues explored here in relation to the OSOR maps released by Global News presented when an interactive map was published showing the names and addresses of registered gun owners in two New York counties. Beyond the privacy concerns, a major issue with the release of the map related to the inadequacy of the metadata and the potential for the public to be misled or even endangered by the inaccuracies in the information. The errors resulted from many factors, including deaths and changes of residences that were not updated in the registry itself (Scassa, "Privacy," *supra* note 12 at 403–404; Abby Rogers, "New York Newspaper Accused of Posting Inaccurate Gun Map As Gun Permit Applications Soar," *Business Insider* (9 January 2013), online: <www.businessinsider.com/inaccuracies-in-journal-news-gun-map-2013-1>; Laura Incalcaterra, "Many handgun permits in N.Y. county have outdated data" *USA Today* (27 January 2013), online: <www.usatoday.com/story/news/nation/2013/01/27/outdated-new-york-gun-permit-data/1868787/>.

140 Janssen, Charalabidis & Zuiderwijk, *supra* note 41 at 264.

141 Note that the data made available for download by the public from the Global News website is in excel format and contains little accompanying metadata.

142 Kitchin, *Data Revolution*, *supra* note 1 at 134–35; Kitchin & Lauriault, *supra* note 2; Janssen, Charalabidis & Zuiderwijk, *supra* note 41 at 264–65 (discussing bias in data that arises due to underlying assumptions made in the collection phase and noting that, because data always gives an incomplete picture, it is crucial to always ask what information a given data set conceals).

143 Canada, "Open Data Roundtables Summary Report," by David Eaves, online: <open.canada.ca/en/open-data-roundtables-summary-report> ["Roundtables Report"]. The need for standards for metadata in the open data context has been emphasized elsewhere: see e.g. Committee on Government Operations, *supra* note 108 at 9 (emphasizes the need for standards in order to allow users to assess whether data released by different jurisdictions is comparable).

144 Committee on Government Operations, *ibid* at 10. An option suggested as part of the round table discussions was to adopt what is known as the "Dublin Core Metadata Standard" (DCMS), which involves use of the following fifteen elements to describe an information resource: contributor (e.g. a person, organization, or service responsible for contributing to the resource); coverage (e.g. spatial or

of metadata that should be required, round table discussions hosted by the federal government emphasized the need to assist lay people to understand the limits of government data sets. Among other things, metadata should include details of the purposes for which the data was collected and contact information for the government employee who created or controls the information.[145] This discussion corresponds to the argument that, in the open data context, emphasis must be placed on the "chain-of-custody" so that users have the opportunity to trace the information back to its source in order to understand its limitations.[146]

Proper metadata could assist new users of data disclosed in the proactive disclosure and open data contexts in determining whether a planned secondary use of data is consistent with the nature and limitations of the data set. Because users of government information may not be experienced researchers, this effort should be accompanied by a long-term commitment to promoting digital literacy among the general public, for instance within the public education system.[147] The Canadian government has indeed expressed its commitment to improving data literacy among Canadians, starting with the provision of training materials and online tools as part of the open government initiative.[148]

## V. BALANCING TRANSPARENCY AND PRIVACY

In the access to information, proactive disclosure, and open data contexts, the issue of identifiability (and thus, whether information should be considered personal information) will need to be balanced against the goals of government transparency and accountability. The balance between transparency and privacy is likely to be increasingly engaged as federal, provincial, and municipal governments move towards open data and proactive disclosure as part of broader open government programs.[149]

The more ready a decision-maker is to find that anonymized data sets can lead to the re-identification of individuals, the less likely information is to be disclosed. This pits the goal of protection of privacy squarely against that of achieving greater transparency and accountability. In *Community Safety and Correctional Services*, the Supreme Court of Canada accepted the narrower approach to re-identification risk put forward by the adjudicator. As demonstrated above, key features of this approach include: (1) the party seeking to avoid disclosure on the basis of re-identification risk must be able to connect the

---

temporal topic or applicability of the resource, jurisdiction in which the resource is relevant); creator (e.g. a person, organization, or service primarily responsible for creating the resource); date; description (e.g. an abstract or table of contents); format (relates to format medium or file dimensions); identifier (resource information); language; publisher; relation (e.g. a relationship to other resources); rights (e.g. intellectual property rights over the resource); source (from which the resource is derived); subject (which may be represented by keywords or phrases); title; and type (e.g. the genre of the resource): see Dublin Core Metadata Initiative, "Dublin Core Metadata Element Set, Version 1.1," online: <dublincore.org/documents/dces/>. Note that this list provides basic and abbreviated information about the DCMS. To implement the standard, reference to a complete description of the initiative would be required. See also "Roundtables Report," *ibid*.

145 "Roundtables Report," *ibid*.

146 Ontario, Information and Privacy Commissioner, "Privacy and Government 2.0: The Implications of an Open World," by Ann Cavoukian (Toronto: OIPC, May 2009) at 5.

147 See e.g. British Columbia, Information and Privacy Commissioner, *Investigation Report F13-03: Evaluating the Government of British Columbia's Open Government Initiative*," by Elizabeth Denham (Victoria: BCIPC, 25 July 2013) at 36, online: <www.oipc.bc.ca/investigation-reports/15537>.

148 "Canada's Action Plan," *supra* note 6. Note, however, that digital literacy (as discussed in the Action Plan) is not necessarily the same as data literacy.

149 Kulk & van Loenen, *supra* note 63 at 203–204.

dots between the data sought for disclosure and other data sets that can lead to the re-identification of individuals; (2) speculation about the risk of re-identification in the abstract is insufficient and the risk must be demonstrated on a balance of probabilities in light of the data at issue; and (3) the spectre of future re-identification is disregarded as too speculative. In other words, the fact that more and more data may soon be available, or that more powerful analytic tools may be developed, or that private actors may have their own collections of data that can lead to re-identification, are, in general terms, irrelevant to the evaluation of re-identification risk.

The Court's acceptance of the narrower approach to assessing re-identification risk in *Community Safety and Correctional Services* and the potential application of this approach to open data and proactive disclosure of information are considered here in relation to three issues. The first is the purpose-driven approach to restricting secondary uses of information that has played a central role in Canadian privacy and data protection laws. This approach appears relevant to the open data and proactive disclosure movements and may need to be given a more prominent role in the decision-making process relating to disclosure of new data. The second issue is the question of how government actors should proceed in assessing re-identification risk given the acceptance of a narrow view of the test taken by the Supreme Court in *Community Safety and Correctional Services*. Finally, in an effort to reflect the need to balance the privacy issues emphasized in this article and the important value of transparency, situations that may lean more towards disclosure will be examined.

### A. PURPOSE-DRIVEN APPROACH

It is suggested that some other considerations may be relevant to governments in establishing a balance between transparency and accountability, whether it be in the context of access to information, proactive disclosure, or open data. These reflect the concerns outlined in Parts III and IV of this article, and are part of what we call a purpose-driven approach. Fundamentally, such an approach considers the purpose for the collection of the data in the first place in order to search for guidance as to whether and to what extent such data should be disclosed proactively or as open data. For example, when requests are made for information collected in accordance with a program like the OSOR, the enabling legislation relating to the collection of the data at issue might indicate a clear public policy choice regarding transparency in the legislation or its regulations. As previously discussed, the information contained on the OSOR has never been made available to the public. The withholding of information from the public in this case was a clear policy choice based on the needs of the program, which is clearly reflected in *Christopher's Law*.[150] If, as in *Community Safety and Correctional Services*, privacy or confidentiality is a clear value reflected in the enabling legislation, it might be argued that this should shift the balance more towards privacy than disclosure when it comes to decisions about the release of information relating to the government program. Admittedly, the withholding of information based on speculative concerns or a policy of erring on the side of caution would conflict with the prevailing view within the open government and open data movements that publicly-held

[150] The statute prohibits disclosure of the information by persons with access to the OSOR except in very limited circumstances in which the information is communicated to other law enforcement agents for the purposes of crime prevention (*supra* note 27, s 10).

information should be open by default.[151] At the same time, the decision to disregard these more speculative concerns is itself a policy choice. The issue could potentially be dealt with by incorporating a sliding scale that acknowledges the policy choices relating to individual privacy as well as the need to promote transparency within government. By assessing requests for disclosure in this light, courts could contemplate both issues as important public values from a perspective that might lead to a more open discussion about the balance to be obtained in the access to information and open data context, especially as information technologies continue to advance and the privacy issues continue to become increasingly complex.

Purpose for collection is an important privacy principle when it comes to limiting the reuse of personal information for secondary purposes. For instance, the federal *Privacy Act* requires that government institutions inform individuals from whom they collect information of the purpose for which the information is being collected and that they obtain fresh consent from those individuals for uses beyond or inconsistent with that purpose.[152] Similarly, the *Personal Information and Protection of Electronic Documents Act* provides that private organizations can "collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[153] In the current context, the purpose for collection principle requires consideration of whether the release of information to the public is consistent with the purpose for which it was collected. In a general sense, Kitchin emphasizes the need "to be mindful that government data is generated

---

151 See Committee on Government Operations, *supra* note 108 at 5; "G8 Open Data," *supra* note 7; "Open by Default," ON, *supra* note 108; "Open Data Policy" AB, *supra* note 108.

152 *Privacy Act*, *supra* note 51, ss 5(2), 7(a). Note that section 7(b) allows specific uses of information outlined in section 8(2) of the *Act* without requiring individual consent (for instance law enforcement purposes such as complying with a subpoena or warrant issued by a court, internal audit purposes, or disclosure to Library and Archives for archival purposes).

153 *PIPEDA*, *supra* note 62, s 5(3). This focus on the purpose for which information has been collected is also relevant in other legal contexts, including in healthcare treatment and research. Canadian courts have held that secondary uses for information disclosed in the treatment context require fresh consent because information disclosed to healthcare providers is viewed as being subject to an understanding that consent for use is limited to purposes relating to treatment only. See e.g. *R v Dyment*, [1988] 2 SCR 417 (where the Court determined that the unauthorized use of a patient's blood sample for law enforcement purposes was an infringement of the patient's right to a reasonable expectation of privacy under section 8 of the *Charter*). The introduction of electronic health records has been accompanied by reminders that Canada's privacy laws reinforce the patient's right to control access to and reuse of personal health information, even in relation to healthcare providers who treat the patient in the future and who may have an interest in accessing a patient's health record for the purposes of that treatment: see Nola M Ries, "Patient Privacy in a Wired (and Wireless) World: Approaches to Consent in the Context of Electronic Health Records" (2006) 43:3 Alta L Rev 681. The purpose-driven approach is not always easy to maintain in this context, acting as a burden on researchers to the extent that they need to obtain consent for each new use of information collected for research purposes. Still, the option of moving to an opt-out model as a replacement for the traditional requirement of consent has been heavily criticized as a departure from the protection of individual privacy and autonomy afforded by the requirement for specific consent for each new use of personal information: see Timothy Caulfield & Bartha Maria Knoppers, "Consent, Privacy, & Research Biobanks: Policy Brief No 1," (Ottawa: Genome Canada, 26 January 2010) at 5, online: <www.genomecanada.ca/medias/pdf/en/GPS-Policy-Directions-Brief.pdf>. See also Nola M Ries, "Research with Blood Donated to Blood Banking Organizations" (2013) 21:2 Health L Rev 5, which examines the secondary research use of blood donated for medical purposes and advising blood service organizations to obtain consent for uses of blood samples in research. The author notes, at 9, that a Canadian class action lawsuit is currently underway that relates to the unauthorized retention and use of blood samples taken from newborns for medical screening purposes (*ibid* at 9). See *D (L) (Guardian ad litem of) v Provincial Health Services Authority*, 2011 BCSC 628, 234 CRR (2d) 84; *LD v Provincial Health Services Authority*, 2012 BCCA 491, 331 BCAC 43. The difficulties in maintaining the purpose-driven approach is a matter that will likewise need to be debated in the open government and proactive disclosure contexts, where the issue is likely to become equally relevant.

for the purposes of governance."[154] While the release of information that supports greater transparency in relation to government operations is arguably consistent with that initial purpose, this is not necessarily the case if greater transparency in government is not a likely outcome of disclosure.

### B. RE-IDENTIFICATION RISK

A second issue is the likelihood that the information disclosed could lead to the identification of specific individuals if and when it is combined with other available information. As Ohm has demonstrated, re-identifcation risk is real and is constantly increasing.[155] It may be very difficult for a public body to identify data sets or analytic tools relevant to the re-identification risk in a particular case given their more limited resources and expertise in these areas. This conflict introduces several important questions in terms of the degree of effort required by government actors to ensure protection of privacy. Will it suffice simply to proactively disclose anonymized data or to release it as open data without carrying out an analysis of the likelihood of re-identification? Will it be possible for an individual who is later identified from information disclosed by a public organization to establish *ex post facto* that the re-identification risk was sufficiently obvious to require non-disclosure? To fully appreciate these risks, the courts may need to consider extending the role of expert evidence and scholarly research beyond what was permitted in *Community Safety and Correctional Services* — both in the access to information context in which that case was decided and in the developing open government and proactive disclosure contexts. In the decision-making process around the release of open data or the proactive disclosure of government information, privacy impact assessments are being incorporated to help clarify some of the risks.[156] Other key issues will be the level of support and guidance provided to bureaucratic decision-makers in these contexts, as well as the methodology developed for assessing re-identification risk. If there is a risk of re-identification associated with the release of the data, decision-makers should consider using appropriate anonymization techniques.[157] As discussed above, anonymization of data does not eliminate all risk of re-

---

154 Kitchin, *Data Revolution*, *supra* note 1 at 63.

155 *Supra* note 22.

156 A Privacy Impact Assessment (PIA) has been defined as "a process used to determine how a program or service could affect the privacy of an individual", which can "help to avoid or lessen possible negative effects on privacy that might result from a program or service" (Canada, Canada Revenue Agency, "Privacy Impact Assessment," online: <www.cra-arc.gc.ca/gncy/prvcy/pia-efvp/menu-eng.html>). Former Privacy Commissioner of Canada Jennifer Stoddart has emphasized the need to use PIAs in the open government context "as building blocks for planning and design rather than being treated as afterthoughts, add-ons, appendices or boxes to be checked" (Jennifer Stoddart, "Open Government and the need to balance institutional transparency with individual privacy" (Remarks delivered at the XXVII German-Canadian Conference, 1 October 2012), online: Office of the Privacy Commissioner of Canada <www.priv.gc.ca/media/sp-d/2012/sp-d_20121001_e.asp>). PIAs have been introduced as a central component of open data initiatives (City of Toronto, City Clerk's Office, "Protection of Privacy Policy," Policy No CIMS 006, Version 1.0 (Toronto: City Clerk's Office, 21 July 2014) online: <www1.toronto.ca/City%20Of%20Toronto/City%20Clerks/Corporate%20Information%20Management%20Services/Files/pdf/P/ProtectionOfPrivacyFinalAODA.pdf>), and have been relied upon in the access to information context to highlight potential privacy risks, particularly with respect to 'data-linking initiatives' (British Columbia, Information and Privacy Commissioner, "Early notice and Privacy Impact Assessments to the OIPC under the *Freedom of Information and Protection of Privacy Act*" (Victoria: BCIPC, July 2012)).

157 EC, *Opinion 06/2013 on open data and public sector information ('PSI') reuse* by Article 29 Data Protection Working Party, 1021/00/EN WP207, (Brussels: Directorate of General Justice, 5 June 2013) at 12, online: <ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf> [Article 29 Working Party]; Kulk & van Loenen, *supra* note 63.

identification, but may help to lessen the risks as open data and proactive disclosure efforts continue.[158]

### C. UNPACKING TRANSPARENCY RATIONALES FOR DISCLOSURE

A third consideration is that the rejection of speculative approaches and erring on the side of transparency are clear indicators that transparency will trump privacy unless the risks for identifiable individuals can be demonstrated. The challenge is therefore to develop a principled approach to the release of government information that recognizes the privacy-transparency spectrum and ensures adequate consideration is given to each value.

On the spectrum of transparency, it is arguable that transparency that offers better insight into the operations of government, the spending of public money, and the extent to which government can be held accountable should be given priority over disclosures that are more related to satisfying curiosity, or provoking public debate. It is important to note that in the open government context, the aim is not only to shed light on government operations, but also to make increasingly more data available as a way to encourage innovation.[159] Here, transparency is much less important. The balance is between privacy rights and the economic value of the data, and claims about transparency should not be used to obscure this fact.

Though it is difficult to foresee the advantages that might be derived from data until it is made available to secondary users, the courts have an important role to play in clarifying the reasons for ordering disclosure in disputes like the one in *Community Safety and Correctional Services*. Ideally, clarification will come through developing scholarship on the impact of transparency and accountability initiatives, an area of research that has been identified as a new priority but that is likely to face challenges in terms of measuring impacts that tend to be intangible and difficult to quantify.[160] Clarification of what is meant by transparency represents a key feature of this emerging scholarship. As John Gaventa and Rosemary McGee point out, to be able to discuss the impact of transparency and accountability initiatives in terms of "what they *have achieved* — we need to be clear about their aims, that is, what they *sought to achieve*."[161] As mentioned above within the discussion of the concept of transparency and the information conveyed by the Global News map, both the Supreme Court of Canada and the Information and Privacy Commissioner of Ontario linked the decision in *Community Safety and Correctional Services* to the value of transparency without much analysis of how transparency was actually served through the release of the OSOR information. The above discussion argued that the gains for transparency resulting from the release of the information in *Community Safety and Correctional Services* were limited. Going forward, it would be useful to have more detailed explanations of the expected benefits of specific disclosures, including the potential for the information to serve transparency goals. While decisions to withhold information would still

---

158 See comments in Article 29 Working Party, *ibid* at 5.

159 Certain types of government information may be primarily useful in encouraging innovation rather than serving transparency goals. See e.g. Harlan Yu & David G Robinson, "The New Ambiguity of 'Open Government'" (2012) 59 UCLA L Rev Discourse 178 at 180 (Yu & Robinson point out that bus schedules and restaurant inspection data may be used to offer or improve on certain services, but may not offer a great deal in terms of enforcing government accountability).

160 Gaventa & McGee, *supra* note 105 at s8.

161 *Ibid* at s10 [emphasis in original].

need to be based on principled reasons, it might be easier to accept the withholding of information absent any convincing argument about how the disclosure of information will serve the goals of the open government movement, depending on the context in which the request is made.

## VI. CONCLUSION

In *Community Safety and Correctional Services*, the Supreme Court of Canada endorsed a narrow approach to assessing re-identification risk in the release of government information. With this approach, evidence of identifiability is to be based on the specific data set at issue instead of on speculative risk relating to evolving information technologies and the growing availability of data. To a large extent, the decision is based on the realities of an old data world. The changing data context was not a feature of the decision, and we have argued that it needs to be taken into account. In particular, the narrow view of re-identification coupled with the characterization of the decision as a win for transparency prompts a discussion of the meaning of transparency in the access to information, open data, and open government contexts. *Community Safety and Correctional Services* lacks a clear assessment of either the scope of the transparency principle or the extent to which disclosure in this case actually served transparency goals. It is not evident that transparency automatically results from mere disclosure of information, and the case offers little guidance to those who must balance transparency and privacy in making decisions about proactive disclosure and open data. The problem is made more acute by the fact that there is increasing pressure towards open data and proactive disclosure by governments at all levels in Canada.

Recognizing that both transparency and privacy are important values, we propose some guiding principles to assist decision-makers to strike a balance between transparency and privacy in the open data and proactive disclosure contexts. This guidance is meant to be sensitive to the realities of the big data context. First, the concept of transparency that is part of the balance must be nuanced and meaningful. A clear idea of what is meant by transparency is crucial in order to allow individual decision-makers to weigh the degree of privacy risk against the amount of transparency gained from disclosure of government-held information. Second, re-identification risk should be assessed with regard to the big data context into which the data will be released. In some cases, the risk of re-identification will be outweighed by the transparency value of the data. Where the transparency value is low, it may not justify the risk to privacy. Third, although de-identified data may offer a compromise between transparency and privacy, consideration must be given to whether the data remains meaningful after de-identification. When data is released based on the conclusion that it could facilitate greater transparency in government operations, the likelihood of transparency must be improved by the release of quality data with appropriate and accessible metadata. Finally, to maximize the potential benefits of releasing quality data accompanied by appropriate metadata, steps must be taken to improve not just digital literacy, but also data literacy.

By implementing this approach to assessing information available for release either as open data or through proactive disclosure into the big data environment, civil servants who play a crucial decision-making role will gain a better understanding of the privacy issues at stake. In addition, the process will force a more open discussion about the meaning of

transparency as a goal driving the move towards greater openness in government. By defining and contextualizing the concepts commonly invoked in the rhetoric surrounding the open data and open government movements, a clearer picture of the status of personal privacy in the big data context will emerge.