David Asper Centre for Constitutional Rights
UNIVERSITY OF TORONTO

Submission to the House of Commons Standing Committee on Access to Information, Privacy, and Ethics

Dr. Lisa M. Austin
Associate Professor, University of Toronto Faculty of Law

Tuesday, June 14, 2016

Submission to the House of Commons Standing Committee on Access to Information, Privacy, and Ethics

Introduction

Privacy Act reform must take into account privacy rights under the *Canadian Charter of Rights and Freedoms*.

In the early 1980's, Canada introduced both the *Charter* and the *Privacy Act*. Both protect privacy but the relationship between the two is not always clear and there is little in the current role of the Office of the Privacy Commissioner of Canada that reflects the constitutional dimensions of privacy protection. *Privacy Act* reform must address the two solitudes of privacy law in Canada and bring them into a more robust integration. Compliance with the *Privacy Act*, as it now stands, does not ensure compliance with the *Charter*.

This is all the more important in the current context, where the *Privacy Act* is being pressed into service to protect privacy in relation to national security and law enforcement. For example, when Bill C-51 was introduced by the former government, and with it increased information sharing within government through the *Security of Canada Information Sharing Act*, an official backgrounder document indicated that the *Privacy Act*, and the review provided by the Office of the Privacy Commissioner, "will help maintain an appropriate balance between protecting the privacy of citizens and ensuring national security."[1]The idea that the *Privacy Act* provides the tools to ensure an adequate balance between privacy and national security is dangerously inaccurate.[2]

The *Privacy Act* is quasi-constitutional legislation.[3] However, it should not be equated with the constitutional protection of privacy rights.[4] The *Privacy Act* is based on what have come to be known internationally as "Fair Information Principles". Its model is a response to the growth of the administrative state and its

---

[1] Government of Canada, "Backgrounder: Security of Canada Information Sharing Act", online: Government of Canada <http://news.gc.ca/web/article-en.do?nid=926879&_ga=1.53885867.2078202319.1410971187>.

[2] For a discussion of the relationship between SCISA and the Privacy Act, see Lisa M. Austin, "Anti-Terrorism's Privacy Sleight-of-Hand: Bill C-51 and the Erosion of Privacy" " in Edward M Iacobucci and Stephen J Toope, eds, *After the Paris Attacks: Responses in Canada, Europe, and Around the Globe* (University of Toronto Press, 2015) ["Privacy Sleight-of-Hand"].

[3] *Lavigne v Canada (Office of the Commissioner of Official Languages)*, [2002] SCC 53, at para 24.

[4] For a fuller articulation of the differences between the two privacy paradigms, see Lisa M. Austin, "Towards a Public Law of Privacy: Meeting the Big Data Challenge" (2015) 71 Supreme Court Law Review (2d) 527 ["Public Law of Privacy"]

information practices. An individual seeking government services has an interest in receiving those services and the administration of those services requires personal information to be collected and processed. The individual interest does not lie in preventing this collection, use, or disclosure -- it lies in preventing the over-collection of personal information or its subsequent uses or disclosures for different purposes, as well as in ensuring the information is accurate. The central individual entitlement is to have access to the information the state holds about oneself and to correct for inaccuracies.

The constitutional protection of privacy in Canada has developed largely in relation to s.8 of the *Charter*. Its central paradigm is the search and seizure context where the state seeks information in relation to law enforcement investigations. Here the individual interest lies in *opposition* to the state interest. The central individual entitlement is to have state access protected through the warrant requirement, and the reasonable and probable grounds standard.

The *Privacy Act* was not drafted to deal with the coercive context of law enforcement and national security. As the Office of the Privacy Commissioner of Canada itself has stated: "the antiquated nature of the *Privacy* Act renders it of little significance to the public debate on security and privacy in Canada."[5] Even within the Fair Information Practices paradigm of the *Privacy Act,* many of the protections do not apply in the context of law enforcement and national security due to the exceptions found in the Act.[6]

We are now in an era of increased information sharing within government, and between governments. This information sharing is not in the service of providing the programs of the social welfare state but is for the purposes of law enforcement and national security. The only way that *Privacy Act* reform can address this context is through attention to the *Charter*. When so many of the state's information practices are hidden from the view of Canadians, we need to ensure that these practices are scrutinized for *Charter* compliance when they are being initially implemented and not after the fact. *Charter* compliance needs to be integrated with *Privacy Act* compliance.

---

[5] Office of the Privacy Commissioner of Canada, "Addendum to *Government Accountability for Personal Information: Reforming the Privacy Act*" (2008) at 7, online: <https://www.priv.gc.ca/information/pub/pa_ref_add_080417_e.pdf>.
[6] See Austin, "Privacy Sleight-of-Hand", *supra* note 2.

The Charter Framework

(a) collection of information and Charter right to privacy

Section 8 of the *Charter* protects a "reasonable expectation of privacy" and this is determined according to a variety of ideas including the "totality of circumstances", and whether the information in question is part of an individual's "biographical core".[7]

The idea of "reasonable" in the constitutional context indicates a balancing between privacy and state interests that takes place within s.8 itself. As Justice Dickson outlined in *Hunter v Southam*:

> [t]he guarantee of security from *unreasonable* search and seizure only protects a *reasonable* expectation. This limitation on the right guaranteed by s.8, whether it is expressed negatively as freedom from 'unreasonable' search and seizure, or positively as an entitlement to a 'reasonable' expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.[8]

In most circumstances, this balancing entails that a warrant is required on a standard of "reasonable and probable grounds, established upon oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search."[9] Subsequent cases have allowed for departures from the *Hunter v Southam* warrant standard in special contexts such as border crossings, in exigent circumstances, or where authorized by a reasonable law and carried out in a reasonable manner.[10]

Most s.8 cases concern law enforcement investigations and, when a s.8 violation has been found, the subsequent question is whether the evidence should be excluded at trial. The relationship between s.8 and s.1 of the *Charter* has been rarely explored and the circumstances under which a s.8 violation will be upheld by s.1 are uncertain.

Although the vast majority of privacy jurisprudence under the Charter deals with s.8, there is a clear trend in favour of also protecting privacy within s.7. For example, the Federal Court of Appeal has held that s.7's right to liberty protects

---

[7] The "totality of circumstances" approach was outlined in *R v Edwards*, [1996] 1 SCR 128 at para 45, affirmed in *R v Tessling*, 2004 SCC 67 at para 19; the "biographical core" analysis was outlined in *R v Plant*, [1993] 3 SCR 281.
[8] *Hunter v Southam*, [1984] 2 SCR 145 at 159-160.
[9] *Ibid* at 168.
[10] See Lisa M. Austin, "Information Sharing and the 'Reasonable' Ambiguities of Section 8 of the Charter" (2007) 57 UTLJ 499.

privacy and that this includes a corollary right of access to personal information.[11] The Ontario Superior Court has also held that s.7 includes a right to privacy and used this to strike down adoption legislation.[12] The Supreme Court of Canada has also indicated in many cases that it would include privacy in s.7.[13]

Even where a s.7 privacy right is violated, this can be justified if it is in accordance with the principles of fundamental justice. It is not clear that the violation of a s.7 right that is not in accordance with the principles of fundamental justice can be justified by a s.1 analysis. The Supreme Court has held that the violation of the principles of fundamental justice can only be justified in "exceptional circumstances."[14]

(b) collection of information under the Privacy Act

Section 4 of the *Privacy Act* permits the collection of personal information where that information "relates directly to an operating program or activity of the institution." Although "personal information" is of broader scope than information that attracts a reasonable expectation of privacy under the *Charter*, there will be some collections of personal information that attract *Charter* protection.

The Office of the Privacy Commissioner of Canada argues that s.4 should be amended to include a "necessity" test modeled on the Oakes test for s.1 of the *Charter*.[15] While this would be an improvement upon the current Act, and strengthen its commitment to Fair Information Principles, this is still deficient from a constitutional point of view. What it does is bypass the constitutional questions raised by ss. 7 and 8 of the *Charter* and rushes to a s.1 justification test.

The balancing that takes place within ss.7 and 8 is much stricter than an Oakes-like test with its emphasis on "minimal impairment". For example, the reasonable and

---

[11] *Ruby v Canada (Solicitor General)*, [2000] 3 FC.589 (FCA). But note that on appeal the SCC considered but did not decide this issue. *Ruby v. Canada (Solicitor General)* 2002 SCC 75.

[12] *Cheskes v Attorney General of Ontario*, 2007 CanLII 36387 (ON S.C.)

[13] *Dagg v Canada (Minister of Finance),* [1997] 2 SCR 403 at para. 66; *R. v. Beare* [1988] 2 SCR 87; *Rodriguez v British Columbia (Attorney General)* [1993] 3 SCR 519 (per L'Hereux-Dube J.); *New Brunswick (Minister of Health & Community Services) v G(J)*, [1999] SCR 46; *R. v. O'Connor* [1995] 4 SCR 411; *B(R) v Children's Aid Society of Metropolitan Toronto* [1995] 1 SCR 315; *Morgentaler* (per Wilson J.); *Godbout v Longueiul (City)* [1997] 3 SCR 315; *Blencoe v British Columbia (Human Rights Commission)*, [2000] 2 SCR 307.

[14] *Re BC Motor Vehicle Act* [1985] 2 SCR 486 at 518; *Suresh v Can*. [2002] 1 SCR 3, para. 128.

[15] Office of the Privacy Commissioner of Canada, "Letter to the Standing Committee on Access to Information, Privacy and Ethics" (22 March 2016), online: < https://www.priv.gc.ca/parl/2016/parl_sub_160322_e.asp>.

probable grounds test is one that contemplates that sometimes the state does *not* get access to the information it seeks even if this information is necessary for a law enforcement purpose. Under s.8, "[t]he idea is *not* that privacy must give way so long as it is intruded upon as minimally as possible but that law enforcement goals hold sway only at a particular point marked by the probable effectiveness of reaching that goal."[16] This idea of probable effectiveness is not part of s.1 jurisprudence.[17]

There are circumstances, therefore, where the collection of information authorized by the *Privacy Act* will nonetheless violate the *Charter*. This will not be remedied by a "necessity" test.

(c) subsequent uses and disclosures under the Charter

Just because information has been legitimately collected by the state for one purpose does not mean that the state is free, from a constitutional perspective, to do as it likes with that information. As the Supreme Court of Canada stated in *R v Mills*:

> Privacy is not an all or nothing right. It does not follow from the fact that the Crown has possession of the records that any reasonable expectation of privacy disappears. Privacy interests in modern society include the reasonable expectation that private information will remain confidential to the persons to whom and restricted to the purposes for which it was divulged.[18]

This is not changed by the fact that a law is passed indicating that the government will share information between departments. As the Supreme Court affirmed in *R v Tessling*, "[s]uggestions that a diminished *subjective* expectation of privacy should automatically result in a lowering of constitutional protection should … be opposed. … Expectation of privacy is a normative rather than a descriptive standard."[19] This protection regarding subsequent uses and disclosures is not restricted to "trust-like, confidential, or therapeutic relationships."[20] Disclosures outside of the "the purpose for which it was obtained or a consistent purpose" violate a reasonable expectation of privacy.[21]

---

[16] Austin, "Public Law of Privacy" *supra* note 4.
[17] *Alberta v Hutterian Brethren of Wilson Colony*, [2009] 2 SCR 567 at para. 85 ("a government enacting social legislation is not required to show that the law will in face produce the forecast benefits. … If legislation designed to further the public good were required to await proof positive that the benefits would in fact be realized, few laws would be passed and the public interest would suffer."
[18] [1999] 3 SCR 668 at para108.
[19] 2004 SCC 67 at para 42.
[20] *R v Quesnelle*, 2014 SCC 46 at para 27.
[21] *Ibid* at paras 40-41.

The sharing of information with foreign states can also trigger *Charter* scrutiny. In *R v Wakeling*, a majority of the Supreme Court of Canada agreed that there can be a residual expectation of privacy in lawfully obtained information that is shared for foreign law enforcement purposes. [22]

(d) subsequent uses and disclosures under the Privacy Act

The *Privacy Act* authorizes the use and disclosure of information in circumstances that should trigger *Charter* scrutiny.[23] Some examples include:

- 8(2)(a) – consistent purposes
    - The problem with this is that, as the Office of the Privacy Commissioner of Canada reports, government practice is to interpret this very broadly. An overly broad interpretation of consistent purposes can run afoul of the *Charter* in some contexts.
- 8(2)(b) – for any purpose authorized by an Act of Parliament
    - The problem with this is that the Act might be unconstitutional itself or the authorization for information sharing could be very broad and vague. Information sharing practices consistent with such broad authority could nonetheless run afoul of the *Charter* in some contexts.
- 8(2)(e) – on the written request from an investigative body
    - The problem with this is that where the information attracts a reasonable expectation of privacy, the *Charter* requires a warrant if the state wants access to it for law enforcement purposes.
- 8(2)(m)(i) – where the public interest clearly outweighs the privacy invasion
    - This could run afoul of the *Charter* if this balancing does not take into account how balancing is done under ss.7 and 8 of the *Charter*.
- 8(2)(f) – under agreements or arrangements with other governments, including foreign governments, for law enforcement purposes
    - After *Wakeling*, such disclosures attract *Charter* scrutiny.

The Office of the Privacy Commissioner of Canada recommends that disclosures under ss. 8(2)(a) and 8(2)(f) require written information-sharing agreements.[24] We agree with this recommendation but question why it is confined to these two

---

[22] *Wakeling v United States of America*, 2014 SCC 72. The Court split on its reasons. 6 justices held that lawfully obtained wiretap information retained a reasonable expectation of privacy but they split on the question of whether the Criminal Code framework for sharing this information with foreign authorities was reasonable. One justice held that s.8 is not engaged when information collected for law enforcement purposes is shared for law enforcement purposes.

[23] Section 7 of the Act authorizes the use of personal information without consent for the same purposes for which s.8(2) authorizes disclosures without consent.

[24] *Supra* note 15.

provisions and why a "necessity" requirement is not built into the review of these agreements.

But even with these amendments, the result will be a *Privacy Act* with a stronger commitment to Fair Information Principles, but not a stronger commitment to *Charter* compliance. We recommend that all government information sharing practices be governed by written agreements and that there be an explicit requirement that such agreements be reviewed for *Charter* compliance. This review should be undertaken by the Office of the Privacy Commissioner of Canada. However, given the potential impact on Charter protected privacy rights, such review should be subject to appeal or judicial review on the standard of correctness.

Accuracy

Canadians need only look to the Arar Commission for details of the tragic impact of inaccurate information on fundamental rights and freedoms, especially in the national security context.[25] When we are dealing with contemporary information practices, we need to also look at accuracy in the processing of the information and not simply accuracy of the information being processed. Algorithmic responsibility, in an era of "Big Data" techniques, is an essential means of safeguarding fundamental rights and freedoms.[26]

Section 6(2) of the Privacy Act provides that government institutions have an obligation of accuracy. This section must be reformed to reflect a broader obligation of accuracy. Currently, the scope of the obligation is limited to the "use" of information "for an administrative purpose." Section 3 of the Act defines "administrative purpose" as "the use of that information in a decision making process that directly affects that individual". In the context of broad governmental

---

[25] Commission of Inquiry into the Actions of Canadian Officials in relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Works and Government Services Canada, 2006).

[26] One can also argue that the government has a constitutional obligation to ensure that it has a rational basis for its interventions where those interventions potentially impact Charter rights. A number of scholars commenting on the Supreme Court of Canada decision in *Chaoulli*—which dealt with the issue of wait times and private health care providers—have argued that the government has a constitutional obligation to provide a rational basis for its decisions regarding the allocation of its resources and interventions. See Lorraine E Weinrib, "Charter Perspectives on *Chaoulli*: The Body and the Body Politic" in Colleen M Flood, Kent Roach and Lorne Sossin, eds, *Access to Care, Access to Justice* (Toronto: University of Toronto Press, 2005) 56 and Stanley H Hart, QC, "Arbitrariness, Randomness and the Principles of Fundamental Justice" in *Access to Care, Access to Justice* 505.

information sharing in the national security context, this could leave out the following:

- Disclosures of information, such as disclosures to foreign governments. The Arar Commission very clearly pointed to the dangers of sharing inaccurate information with foreign governments.
- Use of information in investigations. It is not clear that all investigative processes where information may be used will fall into the scope of "administrative purpose."
- Algorithmic responsibility. Legislation like the *Security of Canada Information Sharing Act* provides the foundation for government "Big Data" practices in the context of national security.[27] This raises different accuracy problems than those contemplated when the Privacy Act was drafted over 30 years ago. For example:
    - Information about persons A, B, C, D, … might be used to infer something about person Z. This inference can affect the rights and interests of Z in profound ways and yet the inaccuracy of the information upon which it is based would fall outside the scope of s.6(2).
    - The algorithm used to create an inference might be inaccurate, such as when it incorporates biases. The inaccuracy of algorithms would fall outside the scope of s.6(2).

Conclusion

It is critical that the *Charter* be central in the review of the legislation in an early, ongoing and transparent manner. It is also important that the Privacy Commission have a role to play in the *Charter* review of the information practices of government which are not as open to inspection by the public and which can have profound implications for the privacy rights of Canadians. Privacy legislation alone does not adequately protect these privacy interests without the application of the *Charter*.

[27] Austin, "Privacy Sleight-of-Hand", *supra* note 2.

Summary of Recommendations

1. **The principles of the Privacy Act should include reference to the privacy rights protected by the Canadian Charter of Rights and Freedoms:**

   "The purpose of this Act is to extend the present laws of Canada, including the rights under the Canadian Charter of Rights and Freedoms, 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."

2. **The use or disclosure of personal information for law enforcement, investigative, or national security purposes should be subject to review that reflects the protection of an individual's Charter rights under ss.7 and 8, and not simply be reviewed on a reasonableness or necessity standard.**

3. **The exemptions under ss.7 and 8 of the Act for uses and disclosures of personal information without consent should be subject to Charter review conducted by the Privacy Commission subject to judicial review on the standard of correctness,**

4. **Section 6(2) of the Act should be amended to impose an obligation to ensure the accuracy of any personal information that is used or disclosed by the institution for all purposes. The obligation of accuracy should also apply to methods of information processing.**