

Invading the Mind: The Right to Privacy and the Definition of Terrorism in Canada

Alysia Davies*

THIS PAPER DEALS WITH THE PREDICTIVE CRIME MODEL that was unleashed in the war against terrorism and its implications for the right to privacy in Canada. The paper is divided into four parts. First, it examines the definition of terrorism found in the 2001 anti-terrorism legislation, which includes a motivational element that requires investigators to prove an offence was committed "for a political, religious or ideological purpose, objective or cause." Then it discusses the development and philosophical underpinnings of the right to privacy and the current state of protection for this right under the *Canadian Charter of Rights and Freedoms*, with a particular focus on the nascent privacy jurisprudence under section 7. The paper then lays out a hypothetical scenario based on the application of offences under the anti-terrorism legislation, and demonstrates how the interests that the right to privacy is supposed to protect could be violated by provisions that are based on the terrorism definition. Finally, the paper looks at the direction that *Charter* jurisprudence may need to take in order to protect privacy in the future, looking in particular at the principles of fundamental justice under section 7, their current content, and the need to adapt them to the new technological crimefighting environment.

L'ARTICLE TRAITE DU MODÈLE DE LA CRIMINALITÉ PRÉDICTIONNELLE développé dans le cadre de la lutte contre le terrorisme et de ses répercussions sur le droit à la vie privée au Canada. L'article est subdivisé en quatre parties. La première examine la définition du terrorisme énoncée dans la loi antiterrorisme de 2001, qui comporte un élément motivationnel obligeant les responsables d'enquête à démontrer qu'une infraction a été commise « au nom d'un but, d'un objectif ou d'une cause de nature politique, religieuse ou idéologique ». La deuxième examine l'évolution et les fondements philosophiques du droit à la vie privée et l'état actuel de cette protection en vertu de la *Charte canadienne des droits et libertés*, plus particulièrement en jetant un regard sur la jurisprudence nouvelle en matière de la vie privée fondée sur l'article 7. Troisièmement, l'article présente un scénario hypothétique fondé sur les infractions de terrorisme prévues dans cette loi et démontre comment les intérêts que cherchent à protéger le droit à la vie privée peuvent faire l'objet d'atteintes par la mise en œuvre des dispositions appliquant la définition du terrorisme. Enfin, l'article explore la voie que pourrait devoir suivre la jurisprudence fondée sur la *Charte* afin de protéger dans l'avenir la vie privée, en prêtant une attention particulière aux principes de justice fondamentale énoncés à l'article 7, au contenu de ces protections, et à la nécessité de les adapter au nouveau milieu technologique de lutte contre les infractions criminelles.

Copyright © 2006 by Alysia Davies.

* Alysia Davies is a practising lawyer in Ottawa, Ontario. This paper was completed with the assistance of a publication grant from the University of Toronto Centre for Innovation Law and Policy.

251	1. INTRODUCTION
252	2. THE DEFINITION OF TERRORISM
259	2.1 <i>Attempted Charter-Proofing</i>
261	3. THE OVERLOOKED CHARTER RIGHT: PRIVACY
261	3.1 <i>Philosophical Background</i>
269	3.2 <i>Section 8 of the Charter and the "Biographical Core of Information"</i>
272	3.3 <i>Section 7 of the Charter and the "Biographical Core of Information"</i>
272	3.3.1. Security
273	3.3.2. Liberty
276	3.3.3. Future Developments
279	4. THE DEFINITION, THE RIGHT, AND THE PRINCIPLES OF FUNDAMENTAL JUSTICE
286	5. EXPANSION OF THE PRINCIPLES OF FUNDAMENTAL JUSTICE
295	6. CONCLUSION

Invading the Mind: The Right to Privacy and the Definition of Terrorism in Canada

Alysia Davies

1. INTRODUCTION

THE COMBINATION OF TERRORIST THREATS and new technologies often gives rise to a spy-novel scenario about a high-tech clash of titans, where terrorists armed with mini-bombs and viruses are thwarted by police and intelligence agents who use anticipatory profiling and tracking methods straight out of the movie *Minority Report*. This high-adrenalin plot receives far more attention than another clash involving technology and terrorists—the one between a new ability to invade and analyse people's daily lives as never before and their classic democratic right to live unobserved by the state.

This classic right is more commonly known as privacy, which has historically been protected by rigid social conventions and the logistical impossibility of keeping track of more than a few people at a time. Although the concept of a right to privacy was first articulated at the beginning of the 20th century, it is only starting to come into its own at the dawn of the 21st. Technology now makes it plausible to track, collect, and manipulate information about people's actions, reactions, and even their thoughts, to an extent never previously imagined. Privacy is the natural antidote to an abuse of such power, and has suddenly become a relevant right rather than a latent one. Its confusing philosophical and jurisprudential background has begun to receive scrutiny in the legislatures and the courts as a result.

At the same time, awareness of the terrorist threat so brutally displayed by 9/11 has begun to revolutionize law enforcement. Investigators and anti-terrorist experts are pressing for greater powers to use existing and emerging technologies to gather information, while combining them with a preventive model of crime-fighting designed to ensure that no terrorist is able to replicate the World Trade Center disaster or anything like it. This model has spurred an attempt to create profiles of suspected terrorists that include the political, ideological, and religious beliefs that might motivate them to such actions.

Indeed, collection of this type of data has already come to be considered so integral to anti-terrorist efforts that several major countries in the West, including Canada, rapidly incorporated it into the terrorism legislation passed after 9/11. The new Canadian definition of terrorism includes these categories of belief as an essential element.

The inquiry into the area of political, religious, and ideological belief newly mandated by Canada's *Anti-terrorism Act* (ATA)¹ is likely to become the first test of how well privacy and the predictive crime model can accommodate each other in this country. This paper will examine the Canadian definition of terrorism and its possible application in conjunction with the terrorist offences laid out in the ATA. It will then look at the state of the right to privacy in Canada, and the extent to which this right can respond to the kinds of challenges presented by the terrorism definition.

*

2. THE DEFINITION OF TERRORISM

THE INTRODUCTION OF THE ATA has provided Canada with a comprehensive definition of terrorism for the first time. While the Supreme Court of Canada has propounded a different working definition of terrorism in the *Suresh*² case to be used in conjunction with the *Immigration and Refugee Protection Act* (IRPA)³ in deportation cases,⁴ the ATA definition is the standard one in all other domestic settings.

The ATA definition is controversial because it contains an element which was not included in the terrorism definitions passed by many other countries in the wake of 9/11. Section 83.01(1)(b)(i) of the definition states that terrorism is:

- (b) an act or omission, in or outside Canada,
 - (i) that is committed
 - (A) in whole or in part for a political, religious or ideological purpose, objective or cause, and
 - (B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada

1. *Anti-terrorism Act*, S.C. 2001, c. 41, <<http://laws.justice.gc.ca/en/A-11.7/2187.html>> [ATA] (Amended: *Criminal Code*, R.S.C. 1985, c. C-46, <<http://laws.justice.gc.ca/en/C-46/41584.html>> [Criminal Code]). As the main ATA provisions are amendments to the *Criminal Code*, the references to the ATA and the *Criminal Code* appear interchangeably in this paper.

2. *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1, <<http://scc.lexum.umontreal.ca/en/2002/2002scc1/2002scc1.html>>, [2002] 1 S.C.R. 3 at para. 98 [*Suresh* cited to LexUM/S.C.R.].

3. *Immigration and Refugee Protection Act*, S.C. 2001, c. 27, <<http://laws.justice.gc.ca/en/I-2.5/64755.html>> [IRPA].

4. The *Suresh* definition is based on the definition provided in *International Convention for the Suppression of the Financing of Terrorism*, UN Res 54/109 (9 December 1999), <<http://www.un.org/law/cod/finterr.htm>>.

This portion of the definition could be described as the *mens rea* of terrorism, in that it states the scope of intent that is considered part of the terrorism offence. The definition in section 83.01(1)(b)(ii) then goes on to define the *actus reus* (act) that must arise from this intent for the act to be considered terrorism.

The “act” of terrorism includes causing death or bodily harm through violence, endangering life, or creating a “serious risk” to the health or safety of the public or any segment thereof. It also includes causing “substantial” property damage where this is likely either to result in the aforementioned death, endangerment, or harm to safety and health, or to cause “serious disruption” of an “essential” service, facility, or system. A “conspiracy, attempt or threat” to commit any of these acts (or to do so by omission) is also considered part of the definition.

Together, the *intent* under (i) and the *act* under (ii) of section 83.01(1)(b) constitute “terrorist activity,” and this definition is used to inform a number of other related terms in the *Criminal Code*, including “terrorist group,”⁵ “facilitating terrorist activity,”⁶ and the list of terrorist “entities” that the Solicitor-General has the power to create under section 83.05 of the *Criminal Code*.

Much of the controversy about this definition has centered on section 83.01(1)(b)(i)(A)—the inclusion of “political, ideological or religious purpose, objective or cause” as a necessary element in the *mens rea* of terrorism. This element appears to implicate the rights and freedoms protected by the *Canadian Charter of Rights and Freedoms*⁷ such as freedom of religion,⁸ freedom of belief,⁹ the right of equality before the law,¹⁰ and as will be set forth in this paper, the section 7 right to life, liberty, and security of the person, in the form of privacy.

Kent Roach has argued that the inclusion of political, ideological, and religious motives is a break with traditional Canadian criminal law in that it makes *motivation*, in addition to intent, an element of the crime.¹¹ Normally, a first-degree murder conviction does not require proof that a killer caused death for certain reasons; it requires merely proof that the killing was intentional, for whatever reason. Indeed, Roach and others have argued that this motivational element is not necessary to prove terrorist intent, and that the aims of intimidating the public or compelling a governmental act by violence as laid out in section 83.01(1)(b)(i)(B) would more than suffice for the intent portion of the definition.

5. Also defined in s. 83.01 of the *Criminal Code*, *supra* note 1.

6. *Ibid.* s. 83.19.

7. *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c. 11, <<http://laws.justice.gc.ca/en/charter/index.html>> [Charter].

8. *Ibid.* s. 2(a).

9. *Ibid.* s. 2(b).

10. *Ibid.* s. 15.

11. Kent Roach, “Did September 11 Change Everything? Struggling to Preserve Canadian Values in the Face of Terrorism” (2002) 47:4 *McGill Law Journal* 893, <<http://www.journal.law.mcgill.ca/abs/vol47/4roach.html>> at p. 903 [Roach, “September 11”].

It has even been suggested that the initiation of criminal offences with a motivational element may work against the state's own aims in prosecuting them. As Paul Gilbert has argued:

All states have laws against political offences such as treason.... But these offences, though they may be committed in conjunction with ordinary criminal offences like murder, are separable from them. The political crime model locates the criminal character of terrorism outside of its political motivation. And this reflects the state's disinclination to try terrorists for treason or other political offences. If it did, then the question of the political justification of terrorist acts would be raised. It is important for the state to insist that no question of justification can be raised: terrorist acts, though politically motivated, are to be regarded as never politically justified because they are merely criminal.¹²

It is noteworthy that the *Suresh* definition of terrorism, the only other one used in the Canadian context, concentrates on intent and act without any mention of motivational underpinnings, except for the specific purposes also found in section 83.01(1)(b)(i)(B) of the *Criminal Code* definition:

...“terrorism” in s. 19 of the Act includes any “act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act”.¹³

While there has not been much jurisprudence on the ATA definition so far, it has been referred to indirectly in IRPA-related cases. In *Ali v. Canada (Minister of Citizenship and Immigration)*, Mactavish J stated that “reference may also be had” to the ATA definition,¹⁴ but then went on to state that any departure from the *Suresh* definition in an IRPA determination is a reviewable error.¹⁵ In *Alemu v. Canada (Minister of Citizenship and Immigration)*, Layden-Stevenson J reiterated that the *Suresh* definition is the standard, but “[f]urther guidance” may be available from the ATA definition.¹⁶

Any reference to the ATA definition in this context would be important, since IRPA applies a lower standard for finding that someone is a terrorist than most of the anti-terrorism legislation. A “reasonable grounds to believe” standard, which is less stringent than the balance of probabilities standard,¹⁷ is

12. Paul Gilbert, *Terrorism, Security and Nationality: An Introductory Study in Applied Political Philosophy* (New York: Routledge, 1994) at p. 49.

13. *Suresh*, *supra* note 2 at para. 98.

14. *Ali v. Canada (Minister of Citizenship and Immigration)*, 2004 FC 1174, <<http://decisions.fct-cf.gc.ca/en/2004/2004fc1174/2004fc1174.html>><<http://decisions.fct-cf.gc.ca/fct/2004/2004fc1174.shtml>>, [2005] 1 F.C. 485 at para. 58.

15. *Ibid.* at para 63.

16. *Alemu v. Canada (Minister of Citizenship and Immigration)*, 2004 FC 997, <<http://decisions.fct-cf.gc.ca/en/2004/2004fc997/2004fc997.html>> at para. 32.

17. *Chiau v. Canada (Minister of Citizenship and Immigration)* (FCA 2000), [2001] 2 FC 297, <<http://reports.fja.gc.ca/en/2000/2001fc27907.html/2001fc27907.html.html>> at para. 60.

applied to determine if a person is inadmissible to Canada on this ground under section 34(1)(c) of the new IRPA¹⁸ and should be deported. The Federal Court of Appeal noted in *Charkaoui v. Canada (Minister of Citizenship and Immigration)*¹⁹ that this standard is constitutionally acceptable provided it is read, as per *Suresh*, as a reasonable belief in a real and serious possibility of adverse effects to Canada.²⁰ This decision is currently under appeal to the Supreme Court.

Outside the immigration context, the general standard to be used for the ATA definition is that of proof beyond a reasonable doubt, but there are some exceptions that apply depending on the stage of the proceedings. For example, a judge can compel testimony in an investigative hearing under section 83.28 if he or she has a reasonable belief that (1) there is an ongoing or imminent terrorist activity, and (2) the witness in question has relevant information.²¹ The Supreme Court of Canada recently found that these procedures did not violate the right to self-incrimination under section 7 of the *Charter* in *Re Application Under s. 83.28 of the Criminal Code*,²² although, as will be discussed later in this paper, it did not analyse or discuss the privacy right under section 7.

The reasonable belief standard is also applied to the police determination of whether there is imminent "terrorist activity" that justifies a preventive arrest and detention under section 83(3)(4). If this is met, then the standard used to identify the potential terrorists or accomplices is the least stringent of all—reasonable *suspicion* that arresting and/or detaining them will prevent the terrorist act is all that is required.²³

Stanley Cohen, who was involved with the drafting of the ATA, has stated that since the terrorism definition requires the presence of motivation, intent, and act together, it is harder to establish terrorist activity than it is to establish traditional criminal offences. He has described the "political, religious or ideological" phrase as "words of limitation."²⁴ It is argued that this distinguishes terrorism from other *Criminal Code*²⁵ acts and helps to justify the lower standards of proof for arrest, detention, and compelled testimony. However, a look at the offences based upon the ATA definition suggests the net cast by the motivational element could actually be much wider in some cases than that of similar criminal offences such as vandalism or murder.

18. IRPA, *supra* note 3, s. 34(1)(c).

19. *Charkaoui v. Canada (Minister of Citizenship and Immigration)*, 2004 FCA 421, <<http://decisions.fca-cf.gc.ca/en/2004/2004fca421/2004fca421.html>>, [2004] 1 F.C. 451.

20. *Ibid.* at paras. 103–107.

21. Martin L. Friedland, "Police Powers in Bill C-36" in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2002) 269–285 at p. 276 [Friedland, "Police Powers"].

22. *Re Application under s. 83.28 of the Criminal Code*, 2004 SCC 42, <<http://scc.lexum.umontreal.ca/en/2004/2004scc42/2004scc42.html>>, [2004] 2 S.C.R. 248 [*Re Application under Section 83.28* cited to LexUM/S.C.R.].

23. Friedland, "Police Powers," *supra* note 21 at p. 279.

24. Stanley Cohen, "Safeguards in and Justifications for Canada's New Anti-terrorism Act" (2002-2003) 14:1 *National Journal of Constitutional Law* 99 at p. 121.

25. *Criminal Code*, *supra* note 1.

Many of the offences relate to membership in, or assistance of a “terrorist group,” which is defined in section 83.01 as:

- (a) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or
- (b) a listed entity,

and includes an association of such entities.

It is important to note that in (a), “terrorist activity” need only be one of the purposes carried out by a group in order for it to be labelled “terrorist.” In the context of targeted investigations within the Muslim community, this may mean that the mostly peaceful congregation of an imam at a particular mosque could be labelled a terrorist group. So could the fundraisers for a prominent cultural or refugee assistance association that has ties to shadowy enterprises which most of its members know nothing about.

The provisions concerning listed entities in (b) increase this likelihood. Section 83.05 of the *Criminal Code* allows the federal government to establish a list of terrorists, on which any group of people can be placed by the Solicitor-General. Again, the only standard of proof involved is reasonable belief. If the Solicitor-General decides on this basis that a group has been involved in terrorist activity or that it is acting “on behalf of, at the direction of or in association with” terrorists,²⁶ it can be added to the list.

Being listed can have dire consequences for the group, including the immediate freezing of its assets and/or seizure of its property at the request of the Attorney-General under section 83.14. This activity is not stayed even if the group invokes the available procedures to defend itself.²⁷ So should the Solicitor-General be eventually proven to have made a mistake with regard to a particular group, it may still be too late to meaningfully alter the course of events arising from the listing.

The definition of “terrorist group” has the potential to automatically put members of an organization identified with a particular set of religious, political, or ideological beliefs into a position where they are suspected of violent criminality. When this is combined with the varying standards of proof in some circumstances, and the broad offences based on assistance of terrorist activity, the spectre of criminalized belief raises its head.

One of the assistance-based offences in particular demonstrates this possibility. The offence of facilitation is supposed to consist of “knowingly” facilitating a terrorist activity;²⁸ but section 83.19(2) of the *Criminal Code* states:

- (2) [...] a terrorist activity is facilitated whether or not
 - (a) the facilitator knows that a particular terrorist activity is facilitated;
 - (b) any particular terrorist activity was foreseen or planned at the time it was facilitated; or
 - (c) any terrorist activity was actually carried out.

26. *Ibid.* s. 83.05(1)(b).

27. These consist of an application to be de-listed under s. 83.05(2) of the *Criminal Code*, possible judicial review under s. 83.05(5) of the *Criminal Code* in the event of a refusal, and/or a “mistaken identity” application under s. 83.07 of the *Criminal Code*.

28. *Criminal Code*, *supra* note 1, s. 83.19(1).

No definition of “facilitation” is provided in the ATA, nor is there reference to any pre-existing definition in the *Criminal Code*. Not only is this a terrorism-based offence that is essentially undefined, but this section appears to remove both the act and a large degree of intent from the offence, which would provide prosecutors with the opportunity to focus mostly on motivation in securing a conviction. It would also give the police an incentive to focus on motivation in gathering evidence, and thus open up lines of inquiry that could not necessarily be justified were the terrorism definition confined only to the specific purposes in section 83.01(1)(b)(i)(B).

This is particularly important because the preventive arrest of a suspected facilitator can be made on thin grounds. As far as the motivational component is concerned, a police officer would only need to “reasonably” believe that a particular religion, political view, or ideology is behind a purported terrorist activity, and to “reasonably” suspect that it is held by a particular “facilitator,” in order to arrest and detain them. If the suspect is somehow associated with an entity listed as a “terrorist group,” then there is no need to believe or suspect anything; an arrest could conceivably be made on the basis of membership alone.

Once someone is picked up on an offence under the ATA, they are subject to far-reaching stigma even if they are not convicted, and they receive considerably fewer procedural protections than an ordinary accused. If convicted, they may be subject to much heavier punishment than they would be for a parallel criminal offence, even in cases where motivation is perhaps the most marked difference between their act of property damage or violence and a run-of-the-mill crime.²⁹

In cases where motivation does become key to obtaining a conviction for terrorist-related activity, there is the question of how it can be proven, especially where a reasonable doubt standard applies. If accused terrorists know it is an essential component of the case for convicting or deporting them, then they may disclaim all political, religious, or ideological motives. Countering this assertion would require investigation into the accused’s thoughts, practices, and opinions, and may of necessity draw police, prosecutors, and investigating judges into imputing beliefs in the face of denial. It is here that considerations of privacy start to come into play.

The motivational component of the ATA definition encourages the invasive collection of broad evidence concerning the ideas and belief systems of individual suspects. At the same time, the ATA amendments to the *Criminal Code* have loosened the traditional requirements for some forms of evidence-gathering, particularly electronic surveillance. A warrant for the interception of communications under Part VI of the *Criminal Code* (titled “Invasion of Privacy”) cannot usually be obtained without a sworn affidavit³⁰ that shows, to the judge’s satisfaction,³¹ that it is an investigative “last resort” after other methods have

29. Kent Roach, “The Dangers of a Charter-Proof and Crime-Based Response to Terrorism” in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom: Essays on Canada’s Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2002) 131–147 at pp. 132–133 [Roach, “Charter-Proof”].

been tried, or that the circumstances are urgent.³² The ATA has exempted terrorism investigators from meeting this requirement,³³ theoretically freeing them up to apply for a warrant as soon as they can assemble enough facts about motivation, intent, and act to swear that they believe activities such as wiretapping would be germane to their investigation.³⁴

It should be noted that many terrorism definitions in other countries do not contain the motivational component, including the one used by the United States of America. The USA PATRIOT Act's³⁵ definition of "domestic terrorism" lays out a more limited scope of intent in section 2331:

- (5) the term "domestic terrorism" means activities that –
- (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
 - (B) appear to be intended –
 - (i) to intimidate or coerce a civilian population;
 - (ii) to influence the policy of a government by intimidation or coercion; or
 - (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping³⁶

The definition of international terrorism, while focused on acts outside the United States or those which "transcend national boundaries in terms of the means by which they are accomplished,"³⁷ is similar to the domestic definition and also omits the motivational component.

The European description of terrorism is based on the *European Convention on the Suppression of Terrorism*³⁸ which was signed by the Council of Europe in 1977. The EU's *Proposal for a Council Framework Decision on Combating Terrorism*, issued in December 2001, stated that in accordance with the *Convention*, "terrorist offences cannot be regarded as a [sic] political offences or as offences connected with political offences or as offences inspired

30. *Criminal Code*, *supra* note 1, s. 185(1).

31. *Ibid.* s. 186(1).

32. *Ibid.* ss. 185(1)(h), 186(1)(b).

33. *Ibid.* ss. 185(1.1)(c), 186(1.1)(c).

34. The pre-existing requirement in s. 186(1)(a) of the *Criminal Code* that the judge must be satisfied that the issuance of such a warrant would be in the best interests of the administration of justice is still applicable to terrorism investigations.

35. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001), <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3162enr.txt.pdf> [PATRIOT Act].

36. 18 U.S.C. s. 2331 (2001), <<http://uscode.house.gov/download/pls/18C113B.txt>>.

37. *Ibid.*

38. *European Convention on the Suppression of Terrorism*, 27 January 1977, E.T.S. No. 90, <<http://conventions.coe.int/Treaty/EN/Treaties/Html/090.htm>>.

by political motives.”³⁹ The final Framework Decision, adopted in June 2002, contains a terrorism definition which does refer to the political implications of certain kinds of intent, but avoids the broad inchoate terminology of political “belief,” “motive,” or “purpose”:

1. Each Member State shall take the necessary measures to ensure that the intentional acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:

- seriously intimidating a population, or
- unduly compelling a Government or international organisation to perform or abstain from performing any act, or
- seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation,

shall be deemed to be terrorist offences.⁴⁰

Western countries which do use an explicit motivational element in their definitions of terrorism include Australia⁴¹ and the United Kingdom⁴² (which does not have a written constitution). It is interesting to note that these countries have received some of the strongest condemnations of their attitude towards civil liberties in the wake of 9/11. The anti-terrorism apparatus of the United Kingdom in particular has been criticized for ignoring privacy concerns, although the House of Lords stated in *Wainwright v. Home Office*⁴³ that there is no recognized common law right to privacy in Britain.

2.1 Attempted Charter-Proofing

The clear *Charter* implications of including political, ideological, and religious motives in the definition of terrorist activity led to a new section being inserted into the ATA after its initial reading in Parliament. This section was intended to clarify that the terrorism definition was not meant to criminalize certain types of beliefs. Section 83.01(1.1) states:

39. EU, *Proposal for a Council Framework Decision on Combating Terrorism*, [2001] O.J.C. 332 E/17, <<http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:C:2001:332E:0300:0304:EN:PDF>> at para (2).

40. EU, *Council Framework Decision of 13 June 2002 on Combating Terrorism* [2002], O.J.L. 164/3, <<http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:L:2002:164:0003:0007:EN:PDF>>, art. 1.1.

41. *Security Legislation Amendment (Terrorism) Act 2002*(Cth), Sch. 1, <http://www.austlii.edu.au/au/legis/cth/num_act/slaa2002n652002478/>.

42. *Terrorism Act 2000* (UK), 2000, ch. 11, <<http://www.opsi.gov.uk/ACTS/acts2000/20000011.htm>>.

43. *Wainwright v. Home Office*, 2003 UKHL 53, <<http://www.publications.parliament.uk/pa/ld200203/ldjudgmt/jd031016/wain-1.htm>>, [2003] 4 All ER 969, [2003] UKHL 53, [2003] 3 WLR 1137.

(1.1) For greater certainty, the expression of a political, religious or ideological thought, belief or opinion does not come within paragraph (b) of the definition "terrorist activity" in subsection (1) unless it constitutes an act or omission that satisfies the criteria of that paragraph.

As may be seen from the analysis in the preceding section, it is nonetheless quite possible that the "expression" of a belief, religion, or ideology might be found to constitute either a threat or an "act" of facilitation of a terrorist activity. This alone is cause for concern, and makes the legislation vulnerable to a challenge based on the expression-based freedoms in the *Charter*, particularly section 2(a), freedom of conscience and religion, and section 2(b), freedom of thought, belief, opinion and expression.

However, the inclusion of the word "expression" in section 83.01(1.1) implies that the government intends the *Criminal Code* to be applied in accordance with these *Charter* freedoms. The extent to which this exception will prevail in practice, given the broad grants of discretion to various state parties under the *Criminal Code* to arrest, detain, and designate people as terrorists, and to freeze their assets, is uncertain. Yet even if the exception were to function perfectly, there are other *Charter* rights which do not appear to be properly caught by the wording of section 83.01(1.1).

For example, as Sujit Choudhry has discussed, the equality protection in section 15 may be invoked against the ATA terrorism definition in the future if a pattern of arrests, charges, and punitive financial measures that appear disproportionately tied to such factors as religion, cultural background, or non-citizen status begins to emerge from its application.⁴⁴ One of the many dangers of racial profiling is its underlying assumption that certain characteristics are synonymous with particular beliefs, motivations, or intentions, even where the person in question has never expressed such an affiliation.

Although the ATA amended the *Criminal Code* to create new sanctions for hate crimes,⁴⁵ it does not address plain discrimination in any other explicit way. It would seem that where the ATA can be applied in a manner that discriminates against people on the basis of inherent or imputed characteristics, rather than on the basis of overt self-expression, *Charter* issues have not been explicitly addressed. Even so, if an argument against the ATA definition under sections 2(a), 2(b) and 15 of the *Charter* were to succeed, it still would not catch the possible criminalization of imputed (rather than expressed) beliefs based on the mostly non-section 15 grounds of ideology and political belief.

These may be caught by section 7 of the *Charter*, which encompasses a privacy interest that includes the protection of a "biographical core of personal information"⁴⁶ about oneself from the state. Privacy is becoming recognized in Canadian constitutional jurisprudence, although its status as a "right" is still the

44. Sujit Choudhry, "Protecting Equality in the Face of Terror: Ethnic and Racial Profiling and s. 15 of the *Charter*" in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2002) 367–381, <http://www.law.utoronto.ca/documents/Choudhry/equality_terror.pdf> at pp. 367–379.

45. *Criminal Code*, *supra* note 1, ss. 320.1, 430(4.1).

46. *R. v. Plant*, [1993] 3 S.C.R. 281, <<http://scc.lexum.umontreal.ca/en/1993/1993rcs3-281/1993rcs3-281.html>> at para. 20 [*Plant* cited to S.C.R.].

subject of discussion and debate.⁴⁷ Yet this emerging right not only addresses gaps in traditional *Charter* arguments that might be brought against the motivational element of the ATA definition; it also has additional implications for many aspects of the new era of terrorism crime-fighting.

*

3. THE OVERLOOKED *CHARTER* RIGHT: PRIVACY

3.1 *Philosophical Background*

PRIVACY WAS FIRST IDENTIFIED as a separate legal interest in 1890 when Samuel Warren and future American Supreme Court Justice Louis D. Brandeis published an article called the "The Right to Privacy" in the *Harvard Law Review*, with the subtitle: "The implicit made explicit."⁴⁸ The catchphrase in the manifesto of the two justices, "the right to be left alone,"⁴⁹ has become a shorthand definition for privacy as it has evolved into a well-recognized right in American jurisprudence. It is currently considered an aspect of the First Amendment to the United States Constitution, under "freedom of conscience"; the Fourth Amendment, in the form of limits on search and seizure; and the Fifth Amendment, as part of the protection against self-incrimination.⁵⁰ It was even referred to as a freestanding common law right in the important US case of *Griswold v. Connecticut*,⁵¹ which affirmed a couple's right to decide whether or not to use birth control.⁵²

Yet there has been much confusion concerning the recognition of privacy in the evolving case law, and part of the problem is that the commonly used definitions of privacy do not always capture the complicated set of interests embodied in the right. Indeed many commentators, most notably William Prosser⁵³ and Richard Posner,⁵⁴ have argued that privacy is a kind of catch-all term for a set of vaguely related interests that are already covered under other heads, rather than a distinctive right in and of itself. This view tends to derive from the traditional means through which the common law dealt with privacy-related concerns, including the protection of private property, the law of defamation and reputation, and torts such as emotional distress.

The counter-argument has been that privacy is not only a coherent concept in itself, but also an essential condition for preserving an individual's autonomy, liberty, and integrity. Alan Westin, one of the most influential writers

47. Stanley A. Cohen, *The Invasion of Privacy* (Toronto: Carswell, 1983) at p. 54 [Cohen, *Invasion of Privacy*].

48. Samuel D. Warren & Louis Brandeis, "The Right to Privacy" (1890) 4:5 *Harvard Law Review* 193, <<http://www.louisville.edu/library/law/brandeis/privacy.html>> [Warren & Brandeis, "Right to Privacy"].

49. *Ibid.*

50. Ferdinand David Schoeman, "Privacy: Philosophical Dimensions of the Literature" in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 1–33 at p. 10.

51. *Griswold v. Connecticut*, 381 U.S. 479 (1965), <<http://supreme.justia.com/us/381/479/case.html>> at p. 486.

52. Lloyd L. Weinreb, "The Right to Privacy" in Ellen Frankel Paul, Fred D. Miller, Jr & Jeffrey Paul, *The Right to Privacy* (New York: Cambridge University Press, 2000) 25–44 at p. 26.

53. William L. Prosser, "Privacy" (1960) 48:3 *California Law Review* 338, reprinted in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 104–155 [Prosser, "Privacy" cited to Schoemann, *Anthology*].

54. Richard A. Posner, "An Economic Theory of Privacy" in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 333–345.

on the subject of privacy, firmly describes it as a stand-alone right. However, he acknowledges that it has two visible faces, each of which he defined in his seminal work *Privacy and Freedom*.⁵⁵ Interestingly, these definitions align with the two heads connected to the recognition of privacy under section 7 of the Canadian *Charter*.

Westin's first definition, which perhaps is most associated with the "liberty" aspect of privacy, is: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."⁵⁶

Westin's second definition, which fits with the psychological "security" aspect of privacy under section 7, is more sociological in nature and involves a relational component that many writers have noted is unique to privacy. Westin describes it this way: "privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity and reserve."⁵⁷

Westin appears to view privacy as the interplay between an individual's decisions about their interactions with others and the related legal claim of control over self-disclosure:

The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives.⁵⁸

The connection of this continual "adjustment process" to exerting one's liberty was noted by Judge Cobb in the American tort case *Pavesich*:⁵⁹

Liberty includes the right to live as one will, so long as that will does not interfere with the rights of another or of the public. One may desire to live a life of seclusion; another may desire to live a life of publicity; still another may wish to live a life of privacy as to certain matters and of publicity as to others Each is entitled to a liberty of choice as to his manner of life, and neither an individual nor the public has a right to arbitrarily take away from him his liberty.⁶⁰

55. Alan F. Westin, *Privacy and Freedom* (New York: Atheneum Press, 1967) [Westin, *Privacy and Freedom*].

56. *Ibid.* at p. 7.

57. *Ibid.*

58. *Ibid.*

59. *Pavesich v. New England Life Ins. Co.*, 122 Ga. 190, 50 S.E. 68 (1905) as quoted in Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39:6 *New York University Law Review* 962, reprinted in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 157–202 [Bloustein, "Privacy as Human Dignity" cited to Schoemann, *Anthology*].

60. *Ibid.* at p. 187.

Privacy has also been frequently linked to human dignity, an interest which has become a staple of Canadian *Charter* jurisprudence, particularly under section 15.⁶¹ Edward J. Bloustein was one of the first commentators to make this link, and after discussing Cobb J's quote, offered this analysis of privacy's importance in the *New York University Law Review* in 1964:

The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual.⁶²

There are three themes visible in these definitions of privacy that are particularly relevant to the fight against terrorism and the "preventive" crime-fighting methods to which it has given rise. The first is the freedom to explore various ideas, thoughts and/or belief systems without being compelled or assumed to commit to them. The second is freedom from constant observation and monitoring, the "right to be left alone" identified by Warren and Brandeis.⁶³ The third is the freedom to choose whether or not to share intimate information and with whom. A loose examination of how these freedoms are impacted by the ideas underlying the anti-terror campaign reveals how they are three successive stages of the same phenomenon, a continuum of privacy in operation.

The new terrorism legislation passed in almost every Western country since 9/11 has been based on the motto of "everything has changed."⁶⁴ The main difference with law enforcement is a perceived need to stop terrorism before it happens, to anticipate a crime far in advance rather than imposing punishment after it has occurred or trying to interrupt it mid-"attempt" (what Irwin Cotler, Canada's former Minister of Justice, calls the "Prevention Principle").⁶⁵ The self-interest that the Western justice system presumes to underlie human behaviour is not an effective restraint against suicide bombers.

The implications of this viewpoint for the right to privacy are serious. Definitions like those found in the ATA are designed to facilitate predictive law enforcement, the kind that infers future behaviour from highly circumstantial evidence and allows the state to err on the side of caution wherever someone is considered a nascent terrorist. This model of law enforcement is fundamentally at odds with the three aspects of privacy laid out above.

61. *Law v. Canada (Minister of Employment and Immigration)*, [1999] 1 S.C.R. 497, <<http://scc.lexum.umontreal.ca/en/1999/1999rcs1-497/1999rcs1-497.html>>.

62. Bloustein, "Privacy as Human Dignity," *supra* note 59 at p. 188.

63. Warren & Brandeis, "Right to Privacy," *supra* note 48.

64. Roach, "September 11," *supra* note 11 at p. 895.

65. Irwin Cotler, "Terrorism, Security and Rights: The Dilemma of Democracies" (2002) 14:1 *National Journal of Constitutional Law*, Special Issue 13 at p. 23.

The freedom to explore ideas is the first, most obviously affected freedom. Where a suspected terrorist does not openly admit to a given set of religious, political, or ideological beliefs, commitment to such beliefs will have to be inferred from that person's behaviour, companions, hobbies, interests, reading habits, and hangouts instead. While these may be valid avenues of investigation under certain circumstances, they are much less solid than the traditional investigative staples of informant witnesses, financial transactions, and communications documented by using a warrant. They are also based on a much more nebulous set of questions. To take the Muslim community as an example, an investigator might ask: is this person a Muslim? A Muslim fundamentalist? The type of fundamentalist who would die for a cause? Are his/her friends and family also terrorists or facilitators? These questions in many instances require judgment on the basis of appearances.

People whose "optics" do not provide clear answers could be branded potential terrorists and endure the devastating consequences, based on what is seen, heard, and arbitrarily associated with them by an outside observer. Under some of the broad definition and offence combinations in the ATA, people could be implicated even when they do not know what their friends are up to; are not sure about their own religious commitment; are culturally associated with beliefs they do not hold; are talking politics in a social setting to playfully discuss ideas about which they are undecided; are using Arabic terms that have multiple translations; are trying to conform to their family's values for the sake of appearances; are running shady but petty errands for an immigration sponsor out of gratitude; or most especially, are young and still changing their views every day. The discretionary investigative techniques employed in the hunt for terrorists allow such people to be "committed" to terrorism *by the decision of another person*, who may "believe" or "suspect" them to be dangerous, but does not know them to be so and in many cases is interpreting their behaviour across an enormous cultural divide.

In addition to criminalizing people on the basis of imputed belief, such investigations may hamper what would have otherwise become positive civic activity as well. Even an aborted preventive arrest could create a level of fear and stigma in the community that is capable of choking off the half-formed thoughts or beliefs of many people before they can become complete and expressed. The actions of the arresting officer⁶⁶ may be predicated on the erroneous assumption that any expression from certain people or groups will unquestionably be threatening and needs to be controlled. It is not hard to see how the regular use of such pre-emptive enforcement could be damaging to a democratic society.

Such sweeping attributions not only of belief, but of how it will be expressed, are also fundamentally at odds with the whole process by which the birth of ideas and opinions in a society takes place. No one can develop an

66. Under s. 83.3(4) of the *Criminal Code*, the officer does not have to obtain an arrest warrant if he perceives danger to be imminent.

informed view without the liberty to explore and think through various other views first. Very few people, especially those who are born in or have moved to a Western society, remain unswervingly committed to the first opinions they are exposed to in life by parents or caregivers, as their perceptions are shaped by their own continuous experience. To assume otherwise in all but the most clear of circumstances is to deprive them of their status as autonomous adults.

Similarly, to assume that people are potentially guilty because of their apparent affiliation with a particular religion or culture, which the ATA definition could be read as giving authorities the discretion to do, disregards each person's right to form and keep their own views in the privacy of their own mind. In communities that are largely composed of immigrants and refugees, this may be a particularly important right—those who must navigate both old traditions and new influences may regularly shield their thoughts in a veil of privacy to avoid endangering community ties on which they depend. Most external observers would not be equipped to assess this phenomenon accurately.

The justified fear of arbitrary assumptions being made about one's beliefs or opinions is also behind the widespread criticism of any notion of mass Orwellian-style surveillance. The prospect of unavoidable, all-pervasive monitoring by the state invading the privacy of our thoughts, our moments alone, or our intimate encounters with others is instinctively abhorrent. Yet technological developments ranging from neurological imaging⁶⁷ to software that records every keystroke ever made on a personal computer⁶⁸ are rapidly making this possibility feasible. Some of this technology is and will be used in terrorist crime-fighting, especially in observation of individuals and groups under suspicion. If ideology, religion and belief are to be elements of a terrorist offence, then evidence of them will need to be provided where a terrorist denies it or his or her allegiances are unclear.

It has been noted in sociological research how observation alters behaviour. As Westin wrote: "[w]hen a person knows his conduct is visible, he must either bring his actions within the accepted social norms in the particular situation involved or decide to violate those norms and accept the risk of reprisal."⁶⁹ He added that the enforcement of these norms through surveillance is in its extreme "psychologically shattering": "[o]nly those who can sustain an absolute commitment to the ideal of perfection can survive total surveillance. This is not the condition of men in ordinary society."⁷⁰

Stanley Cohen has also remarked on the negative socio-psychological effects of constant observation:

67. "Open Your Mind" *The Economist* (23 May 2002), <http://www.economist.com/displaystory.cfm?story_id=1143317>.

68. Scott Spanbauer, "Fight Back Against Surveillance Software" *PCWorld* (26 February 2004), <<http://www.pcworld.com/howto/article/0,aid,114738,00.asp>>.

69. Westin, *Privacy and Freedom*, *supra* note 55 at p. 58.

70. *Ibid.* at p. 59.

At the same time we value our privacy not only as against the criminal but also as against the unnecessary visitations of the state. We do not wish to live our lives under constant scrutiny. Neither would many among us be prepared, or at least pleased, to be required to identify ourselves on demand, to detail our whereabouts or proposed travel plans, to have our personal correspondence scrutinized or our intimate conversations overheard. These things too, are disruptive of social tranquility. The growth of state surveillance is productive of suspicion and distress. It is a siege of another kind.⁷¹

For those who belong to a community, particularly an immigrant community, which is suspected of harbouring terrorists, knowledge that they are being frequently watched may have the same “chilling” effect on their behaviour as an actual preventive arrest or facilitation charge against one of their number. The potential threat or even the unconfirmed fear of surveillance could have similar effects. As Bloustein has noted: “[h]e who may intrude upon another at will is the master of the other and, in fact, intrusion is a primary weapon of the tyrant.”⁷²

Observation in this charged context, with such a grave potential for punishment if one’s actions are wrongly perceived or interpreted, cannot be considered either neutral or non-intrusive. Those who know or worry that they are under surveillance will operate conscious of the threat of being swooped down upon at any minute. They will share with friends, neighbours, and family the constant sense of being unsafe, and not being considered trusted members of society. Indeed, their human relations could well be altered by this surveillance, with those frightened of facilitation charges breaking off contact with old friends and trying to project the image of remoteness from anyone excessively devout or outspoken, just in case.

The sphere of relationships is another area protected by the right to privacy, and not just because the fear, threat, or actual presence of an all-seeing eye can alter people’s behaviour towards each other. The constant amassing of information that might give clues to religious, ideological, or political opinion by means of mass-scale monitoring would violate the third freedom—the right to choose with whom intimate information is shared.

This sharing of this information is key to establishing relationships of all kinds, and how it is handled is often determinative of whether the connection is a one-sided relationship of power or a mutual and voluntary interaction. Charles Fried has described the phenomenon this way:

Monitoring obviously presents vast opportunities for malice and misunderstanding on the part of authorized personnel. For that reason the subject has reason to be constantly apprehensive and inhibited in what he does. There is always an unseen audience, which is the more threatening because of the possibility that one may forget about it and let down his guard, as one would not with a visible audience. But even assuming the benevolence and understanding of the official audience, there are serious

71. Cohen, *Invasion of Privacy*, *supra* note 47 at pp. 20–21.

72. Bloustein, “Privacy as Human Dignity,” *supra* note 59 at p. 165.

consequences to the fact that no degree of true intimacy is possible for the subject. Privacy is not, as we have seen, just a defensive right. It rather forms the necessary context for the intimate relations of love and friendship which gives our lives much of whatever affirmative value they have.... In order to be a friend or lover one must reveal far more of himself. Yet where any intimate revelation may be heard by monitoring officials, it loses the quality of exclusive intimacy required of a gesture of love or friendship.⁷³

Someone's deepest religious beliefs, private political opinions, or secret devotion to an ideology many would consider strange could all form part of the information a person would choose to share gradually or partially with others, depending on their degree of closeness. The state's power to impute or collect this information at will from private phone conversations, emails, discussions overheard at a club or coffee shop, or even the bugging of someone's home or office gives the state the power to impose a unilateral relationship on the person involved. The state knows about you, or thinks it does; you have no say and do not know your watcher in return.

Jeffrey Reiman has posited that it is not only the exchange of intimate information that creates relationships; it is also the terms under which this exchange takes place. He states that "intimacy is not merely the sharing of otherwise withheld information, but the context of caring which makes the sharing of personal information significant."⁷⁴ He adds: "Necessary to an intimate relationship such as friendship or love is a reciprocal desire to share present and future intense and important experiences together, not merely to swap information. Mutual psychoanalysis is not love or even friendship so long as it is not animated by this kind of caring."⁷⁵

His analysis sheds light on why the invasion of privacy can damage human dignity in the relational context. When a person is compelled to share intimate information with someone who does not care about them, who does not have their best interests at heart, and who may seek to use the information against them or may observe it with clinical detachment or distaste, they are being forced into a degrading relationship rather than an intimate one. This is true whether the information is elicited by force, trickery, or merely collection behind one's back.

Another aspect of the connection between privacy and the freedom to experience intimacy may be particularly relevant in the post-9/11 atmosphere. Robert S. Gerstein has commented on the relationship which is perhaps behind the old Christian saying: "That's between a man and his God."⁷⁶ He examines

73. Charles Fried, "Privacy" (1968) 77:3 Yale Law Journal 475, reprinted in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 203–222 at p. 216 [Fried, "Privacy" cited to Schoeman, *Anthology*].

74. Jeffrey H. Reiman, "Privacy, Intimacy, and Personhood" (1978) 6:1 *Philosophy and Public Affairs* 26, reprinted in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 300–315 at p. 305 [Reiman, "Privacy and Intimacy" cited to Schoeman, *Anthology*].

75. *Ibid.* at pp. 305–306.

76. Its best-known use may be in "Wall of Separation," Letter from Thomas Jefferson to Danbury Baptists (1 January 1802), reprinted in *Library of Congress Information Bulletin* (June 1998), <<http://www.loc.gov/loc/lcib/9806/danpre.html>>.

how intimate experiences seem to be generated from a state of full subjectivity, of a kind he notes can be felt in religious ecstasy or prayer:

An experience of intimacy is first of all an experience of a relationship in which we are deeply engrossed. It is an experience so intense that it wholly shapes our consciousness and action. We do not understand ourselves to be choosing to do this or that, or to be looking here or there as we choose. Rather, whatever we do, whatever we see, is a product of the experience in which we are taking part.⁷⁷

He adds that the essential nature of this experience is disrupted if the person must maintain awareness of external circumstances or how they look to others: "We become aware of ourselves as observers separate from the object of observation. The fragile unity of the experience is broken."⁷⁸

While it may be difficult for those raised in a secular society to view religious devotion as a form of intimacy or relationship, this understanding could be vital when dealing with a faith-based community, and more particularly, a fundamentalist person or group. Someone of intense faith may not wish to answer questions about the practice of their religion; they may not even feel able to describe the nature of their beliefs, the form their practices take, or the emotions generated by them. A prohibition on non-Muslims entering a mosque during prayer time may have something to do with protecting the private space needed to have solitary or communal subjective experiences.

Privacy, seen through this lens, protects one's capacity for subjectivity. It is thus not surprising that invasion of this privacy, whether through grilling someone about their religious experiences or bugging a mosque, could be perceived as deeply offensive by both Muslims and believers from other religions.

This subjectivity is the common feature of the freedom to develop and weigh potential ideas, to refuse observation, and to experience interpersonal or religious intimacy. These freedoms all speak to the need for a mental or physical space where one can enter a state of pure subjectivity, whether it is in the form of sensation, emotion, reverie, genius, imagination, doubt, self-exploration, love, or spirituality. This type of space, so crucial to one's autonomy, can only be protected by privacy. This is the basis on which privacy can be considered a right.

While this right exists in Canadian jurisprudence, as will be explored below, it has yet to be fully articulated. However, it is clear that the rise of new technologies in combination with the anti-terrorist preventive model of criminal investigation could easily create the circumstances where this right will be fully explored and tested.

77. Robert S. Gerstein, "Intimacy and Privacy" (1978) 89:1 *Ethics* 76 at p. 76, reprinted in Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 265-271 at p. 266 [Gerstein, "Intimacy and Privacy" cited to Schoeman, *Anthology*].

78. *Ibid.*

3.2 Section 8 of the Charter and the “Biographical Core of Information”

The Supreme Court’s first statements on privacy in the context of the *Charter* occurred in 1984 in *Hunter v. Southam Inc.*,⁷⁹ when Dickson J (as he then was) stated that a “reasonable expectation of privacy”⁸⁰ was protected under section 8 of the *Charter*, which guarantees the right to be free from unreasonable search and seizure. The nature of the privacy referred to in this decision appears to be closest to the classic formulation of the “right to be left alone”:

The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by s. 8, whether it is expressed negatively as freedom from “unreasonable” search and seizure, or positively as an entitlement to a “reasonable” expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public’s interest in being left alone by government must give way to the government’s interest in intruding on the individual’s privacy in order to advance its goals, notably those of law enforcement.⁸¹

Dickson J acknowledged that where national security is involved, the standard to be met for obtaining a search warrant would probably be less stringent. However, he stressed that the balancing exercise between state and individual rights must occur before a potential invasion takes place in order to meaningfully safeguard privacy:

That purpose [of section 8] is, as I have said, to protect individuals from unjustified state intrusions upon their privacy. That purpose requires a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place.⁸²

In *R v. Dyment*,⁸³ LaForest J discussed the balance between “societal needs” and law enforcement.⁸⁴ He identified three areas where section 8 privacy protection is likely to be triggered: “those involving territorial or spatial aspects, those related to the person, and those that arise in the information context.”⁸⁵ These refer to the protection of home or other spaces where personal social interactions may occur, the protection of bodily integrity, and the protection of information about oneself. These spheres have been repeatedly referred to in the section 8 jurisprudence ever since, most recently in *R v. Tessling*.⁸⁶ The “reasonable expectation of privacy,” which contains both a subjective and an

79. *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, <<http://scc.lexum.umontreal.ca/en/1984/1984rcs2-145/1984rcs2-145.html>> [*Hunter v. Southam* cited to S.C.R.].

80. *Ibid.* at p. 159.

81. *Ibid.* at pp. 159–160.

82. *Ibid.*

83. *R. v. Dyment*, [1988] 2 S.C.R. 417, <<http://scc.lexum.umontreal.ca/en/1988/1988rcs2-417/1988rcs2-417.html>> [*Dyment* cited to S.C.R.].

84. *Ibid.* at p. 428.

85. *Ibid.*

86. *R. v. Tessling*, 2004 SCC 67, <<http://scc.lexum.umontreal.ca/en/2004/2004scc67/2004scc67.html>>, [2004] 3 S.C.R. 432 [*Tessling* cited to LexUM/S.C.R.].

objective component, is analysed in relation to whichever type of privacy is being invoked.

While these concepts were advanced under the rubric of section 8, the outlines of a section 7 argument also started to be visible in *Dyment*. LaForest J made reference to Alan Westin's work on privacy and took the position that privacy deserved strong protection:

... society has come to realize that privacy is at the heart of liberty in a modern state Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.⁸⁷

However, the concept of privacy continued to be developed under section 8, and the next step was *R. v. Plant*,⁸⁸ where Sopinka J provided a definition of the kind of information that would fit into the personal information aspect of privacy from *Dyment*:

In fostering the underlying values of dignity, integrity and autonomy, it is fitting that section 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.⁸⁹

This "biographical core of personal information" has become a central aspect of the *Charter* jurisprudence surrounding privacy. McLachlin and Iacobucci JJ described what it includes in *R. v. Mills*:⁹⁰ "These privacy concerns are at their strongest where aspects of one's individual identity are at stake, such as in the context of information 'about one's lifestyle, intimate relations or political or religious opinions.'"⁹¹ They concluded that the privacy interest is "very high"⁹² where personal identity related to the biographical core of information is concerned, or an important relationship based on confidentiality (such as a therapeutic one) needs to be protected. This language is clearly relevant to the contents of the ATA definition.

The privacy right under section 8 that protects this "biographical core" is of a procedural nature, and the balancing exercise between the right and law enforcement needs can vary considerably in outcome depending on the exact nature of the procedures involved. In *R. v. S.A.B.*,⁹³ Arbour J found that both the

87. *Dyment*, *supra* note 83 at pp. 427–428.

88. *Plant*, *supra* note 46.

89. *Ibid.* at para. 20.

90. *R. v. Mills*, [1999] 3 S.C.R. 668, <<http://scc.lexum.umontreal.ca/en/1995/1995rcs1-902/1995rcs1-902.html>> [*Mills* cited to S.C.R.].

91. *Ibid.* at para. 80.

92. *Ibid.* at para. 94.

93. *R. v. S.A.B.*, 2003 SCC 60, <<http://scc.lexum.umontreal.ca/en/2003/2003scc60/2003scc60.html>>, [2003] 2 S.C.R. 678.

bodily integrity and informational section 8 privacy rights mentioned in *Dyment* were engaged by the taking of DNA samples, but distinguished a warrant for obtaining DNA from a wiretapping warrant on the grounds that the privacy of third parties is not implicated by the extraction of DNA.⁹⁴

A geneticist might well dispute this conclusion, considering the information about the accused's family, relatives, and ancestry that could be gleaned from such a sample, and the ease with which a hacker could obtain access to it depending on the security and storage methods chosen. As it happens, the *S.A.B.* reasoning may be scrutinized anew in light of the fact that many of the *Criminal Code* offences, including the undefined "facilitation" of section 83.19, are primary offences under the *Criminal Code*,⁹⁵ which means DNA samples must be collected from those convicted of them for the national DNA databank.⁹⁶ As Lisa Austin has noted in her analysis of this issue, the rationale for collecting such samples is usually related to investigation of offences involving sexual assault or violent personal contact, and it has not been made clear how a DNA sample is supposed to assist in catching a terrorist.⁹⁷

Tessling is the most recent example of a balancing exercise tipped by the technical limits of the procedures involved. In *Tessling*, the RCMP arrested a man for running a marijuana grow operation out of his house, a situation they discovered by using FLIR thermal imaging technology to analyze the heat emanating from the building. The police did not obtain a warrant for their surveillance activities, and the accused brought a section 8 challenge to their methods. Binnie J acknowledged that the territorial privacy described in *Dyment* is implicated in this kind of activity, but found it does not constitute a search under section 8 because current FLIR technology cannot show what is going on inside the home in any specific way; it can only detect heat patterns that can be used as the basis for an inference. He specifically stated that any future form of the technology would have to be analyzed separately:

In my view, with respect, the reasonableness line has to be determined by looking at the information generated by existing FLIR technology, and then evaluating its impact on a reasonable privacy interest. If, as expected, the capability of FLIR and other technologies will improve and the nature and quality of the information hereafter changes, it will be a different case, and the courts will have to deal with its privacy implications at that time in light of the facts as they then exist.⁹⁸

As both *Tessling* and *S.A.B.* show, one of the difficulties in assessing emerging technologies used in crime-fighting is that the information they reveal may change or increase as the science behind them develops further. A purely

94. *Ibid.* at para. 54.

95. Lisa Austin, "Is Privacy a Casualty of the War on Terrorism?" in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2002) 251–267 at p. 255 [Austin, "Privacy a Casualty"].

96. *Criminal Code*, *supra* note 1, s. 487.051.

97. Austin, "Privacy a Casualty," *supra* note 95 at p. 256.

98. *Tessling*, *supra* note 86 at para. 29.

procedural analysis that relies on technical distinctions of the type made by Arbour J in *S.A.B.* and Binnie J in *Tessling* can easily become outdated, and there are many questions about how fully the right to privacy can be protected in this rapidly changing context. This is one reason why privacy jurisprudence in Canada may need to shift away from purely procedural considerations and to focus on section 7, and privacy as a substantive right, instead.

3.3 Section 7 of the Charter and the “Biographical Core of Information”

Privacy as a substantive *Charter* right has been developed under two heads: the “security” interest and the “liberty” interest of section 7. The security theory of privacy came first, and although it is certainly still relevant, the liberty theory appears to be emerging as the dominant strain of thought. Both gradually appeared following the importation of section 8 procedural concerns into the section 7 concept of the principles of fundamental justice, a process that began with *Mills*.⁹⁹

3.3.1 Security

In the 1988 case of *R. v. Beare; R. v. Higgins*,¹⁰⁰ LaForest J stated that he had “considerable sympathy” for the view that section 7 incorporates a right to privacy, although he emphasized that such a right would consist only of the “reasonable expectation” of privacy protected under section 8.¹⁰¹ While he examined privacy mostly under the principles of fundamental justice, he also noted that “the concept ‘life, liberty and security of the person’ refers not only to physical but to mental integrity.”¹⁰²

Both the physical and psychological integrity interests protected under section 7 security have come to be linked with privacy. The bodily integrity category of privacy described in *Dyment* easily interlocks with this branch of section 7 security reasoning. McLachlin J (as she then was) observed in her dissent in *Rodriguez v. British Columbia (Attorney-General)*¹⁰³ that: “Security of the person has an element of personal autonomy, protecting the dignity and privacy of individuals with respect to decisions concerning their own body.”¹⁰⁴ Wilson J’s minority judgment in *R. v. Morgentaler*¹⁰⁵ pointed out how a woman’s privacy with respect to abortion could also be encompassed by the section 7 security right:

99. *Mills*, *supra* note 90 at paras. 87–88.

100. *R. v. Beare; R. v. Higgins*, [1988] 2 S.C.R. 387, <<http://scc.lexum.umontreal.ca/en/1988/1988rcs2-387/1988rcs2-387.html>>.

101. *Ibid.* at p. 412.

102. *Ibid.* at p. 395.

103. *Rodriguez v. British Columbia (Attorney General)*, [1993] 3 S.C.R. 519, <<http://scc.lexum.umontreal.ca/en/1993/1993rcs3-519/1993rcs3-519.html>> [*Rodriguez* cited to S.C.R.].

104. *Ibid.* at p. 618.

105. *R. v. Morgentaler*, [1988] 1 S.C.R. 30, <<http://scc.lexum.umontreal.ca/en/1988/1988rcs1-30/1988rcs1-30.html>> [*Morgentaler* cited to S.C.R.].

... security of the person even on the purely physical level must encompass freedom from the threat of physical punishment or suffering as well as freedom from the actual punishment or suffering itself. In other words, the fact of exposure is enough to violate security of the person.¹⁰⁶

The relationship between psychological security and privacy was examined in *Blencoe v. British Columbia (Human Rights Commission)*.¹⁰⁷ Bastarache J reiterated a statement by Lamer CJC in *Morgentaler* that the psychological security component of section 7 is confined to “serious state-imposed psychological stress,”¹⁰⁸ but acknowledged that it would apply where “the state interferes in profoundly intimate and personal choices of an individual,” and that this would be assessed with reference to the individual’s reasonable expectation of privacy.¹⁰⁹ As will be seen, this language might be particularly relevant to both some of the stressful and invasive directions an investigation into personal beliefs could take under the ATA, and to the potential stigma of preventive arrest.

3.3.2. Liberty

The liberty strain of the section 7 privacy analysis is much more fully developed. It was first raised in *Morgentaler*,¹¹⁰ where Dickson CJC acknowledged that the issue of privacy’s place under section 7 of the *Charter* could be relevant to the case but declined to discuss it.¹¹¹ However, Wilson J, in her minority judgment, embarked on a discussion of the scope of the section 7 right which has proven to be highly influential over the long term.

Wilson J stated that the liberty right “guarantees to every individual a degree of personal autonomy over important decisions intimately affecting their private lives.”¹¹² She counted the decision to terminate a pregnancy as being among these in language containing an echo of the subjectivity needs involved in the relationship between “a man and his God,” which are protected by the privacy right. She specifically referred to a woman’s “freedom of conscience”¹¹³ and stated:

It is a decision that deeply reflects the way the woman thinks about herself and her relationship to others and to society at large. It is not just a medical decision; it is a profound social and ethical one as well. Her response to it will be the response of the whole person.

It is probably impossible for a man to respond, even imaginatively, to such a dilemma not just because it is outside the realm of his personal experience

106. *Ibid.* at p. 162.

107. *Blencoe v. British Columbia (Human Rights Commission)*, 2000 SCC 44, <http://www.lexum.umontreal.ca/csc-scc/en/pub/2000/vol2/html/2000scr2_0307.html>, [2000] 2 S.C.R. 307 [*Blencoe* cited to LexUM/S.C.R.].

108. *Ibid.* at paras. 56–57.

109. *Ibid.* at para. 83.

110. *Morgentaler*, *supra* note 105.

111. *Ibid.* at p. 51.

112. *Ibid.* at p. 171.

113. *Ibid.* at p. 176.

(although this is, of course, the case) but because he can relate to it only by objectifying it, thereby eliminating the subjective elements of the female psyche which are at the heart of the dilemma.¹¹⁴

There is a parallel here with the kind of objectification that could take place as a largely white police force attempts to assess the fervour of belief in an unfamiliar religion such as Islam, and the nature of the actions that could derive from it. In such subjective matters as these, it is far too easy for someone to draw the wrong conclusion about something that is outside their own realm of experience.

After *Morgentaler*, the privacy and liberty discussion did not resume until *B.(R.) v. Children's Aid Society of Metropolitan Toronto*¹¹⁵ in 1995. Lamer CJC wrote a strong dissent in this case opining that the section 7 right to liberty was intended to refer only to the protection of physical liberty against arbitrary imprisonment by the state, and not to "the person's spirit, aspirations, conscience, beliefs, personality, or, more generally, the expression or realization of what makes up the person's non-corporeal identity."¹¹⁶

However, the majority of the Supreme Court endorsed the French sense of the word "liberté" as referring to a more all-encompassing right.¹¹⁷ LaForest J said Wilson J's minority judgment in *Morgentaler* "noted that the liberty interest was rooted in the fundamental concepts of human dignity, personal autonomy, privacy and choice in decisions going to the individual's fundamental being."¹¹⁸ He then went on, as had Wilson J, to discuss the more developed American right to privacy, although he did not at this point explicitly declare a similar right to exist in Canada.¹¹⁹

That declaration finally emerged in *R. v. O'Connor*,¹²⁰ very shortly afterwards. As has been noted by Lisa Austin, while the majority and minority in *O'Connor* agreed that a section 7 privacy interest existed under liberty, they did not agree on how it should be balanced against other interests.¹²¹ L'Heureux-Dubé J, writing for the majority, tied together previous jurisprudence to conclude that therapeutic records of sexual assault victims fall within section 7 and stated: "[s]uch items may consequently be viewed as disclosing a reasonable expectation of privacy which is worthy of protection under section 7 of the *Charter*."¹²²

She argued that this expectation, while not "absolute,"¹²³ should be

114. *Ibid.* at p. 171.

115. *B.(R.) v. Children's Aid Society of Metropolitan Toronto*, [1995] 1 S.C.R. 315, <<http://scc.lexum.umontreal.ca/en/1995/1995rcs1-315/1995rcs1-315.html>> [*B.(R.) v. Children's Aid Society of Metropolitan Toronto* cited to S.C.R.].

116. *Ibid.* at p. 347.

117. *Ibid.* at p. 347.

118. *Ibid.* at p. 368.

119. *Ibid.* at pp. 374–375.

120. *R. v. O'Connor*, [1995] 4 S.C.R. 411, <<http://scc.lexum.umontreal.ca/en/1995/1995rcs4-411/1995rcs4-411.html>> [*O'Connor* cited to S.C.R.].

121. Lisa Austin, "Notes" in Lisa Austin, ed., *Information Law: Cases and Materials*, vol. 1 (Toronto: Faculty of Law, University of Toronto, Winter 2004) at p. 25.

122. *O'Connor*, *supra* note 120 at para. 118.

123. *Ibid.* at para. 117.

protected “at the point of disclosure” in criminal proceedings.¹²⁴ She observed that privacy does not inhere in the documents, but in the person to whom they relate, and so any invasion affects the “dignity and self-worth of the individual, who enjoys the right to privacy as an essential aspect of his or her liberty in a free and democratic society.”¹²⁵ She compared the pre-authorization of searches and seizures under section 8 with the protection of privacy from disclosure as part of the principles of fundamental justice under section 7:

In the same way that our constitution generally requires that a search be premised upon a pre-authorization which is of a nature and manner that is proportionate to the reasonable expectation of privacy at issue [references omitted], s. 7 of the Charter requires a reasonable system of “pre-authorization” to justify court-sanctioned intrusions into the private records of witnesses in legal proceedings.¹²⁶

While the court split on L’Heureux-Dubé J’s conclusions about how to balance privacy against the accused’s right to make full answer and defence under section 7, the majority did endorse her recognition of the privacy right under section 7, with Cory J supporting “many of her conclusions pertaining to privacy and privilege.”¹²⁷ McLachlin J (as she then was) agreed with L’Heureux-Dubé J on disclosure as well and added a comment about the need to also weigh the privacy of third parties in the disclosure process.¹²⁸

The scope and the content of the section 7 privacy right under liberty has not been fully elaborated since the important step taken in *O’Connor*, but there have been some attempts. In *Godbout v. Longueil (City)*,¹²⁹ LaForest J, writing for the minority, stated that section 7 “protects within its ambit the right to an irreducible sphere of personal autonomy wherein individuals may make inherently private choices free from state interference.”¹³⁰ He added that this sphere is not “so wide as to encompass any and all decisions that individuals might make in conducting their affairs,” nor would it include “every matter that might, however vaguely, be described as ‘private’.”¹³¹ However, it would protect all matters that are “fundamentally or inherently personal such that, by their very nature, they implicate basic choices going to the core of what it means to enjoy individual dignity and independence.”¹³²

The matters falling within this private sphere of choices have not yet been completely enumerated, but the recent case of *R. v. Clay*¹³³ concluded that the

124. *Ibid.* at para. 119.

125. *Ibid.* at para. 119.

126. *Ibid.* at para. 119 (references omitted).

127. *Ibid.* at para. 189.

128. *Ibid.* at para. 192.

129. *Godbout v. Longueil (City)*, [1997] 3 S.C.R. 844, <<http://scc.lexum.umontreal.ca/en/1997/1997rcs3-844/1997rcs3-844.html>> [Godbout cited to S.C.R.].

130. *Ibid.* at para. 66.

131. *Ibid.* at para. 66.

132. *Ibid.* at para. 66.

133. *R. v. Clay*, 2003 SCC 75, <<http://scc.lexum.umontreal.ca/en/2003/2003scc75/2003scc75.html>>, [2003] 3 S.C.R. 735 [R. v. Clay cited to LexUM/S.C.R.].

activity of smoking marijuana in one's home does not fit into the category of fundamental and important "personal" decisions that are part of this sphere. However, Gonthier and Binnie JJ, writing for the full court, did endorse LaForest J's minority view in *Godbout* that the section 7 liberty right "is thought to touch the core of what it means to be an autonomous human being blessed with dignity and independence."¹³⁴

The question of whether decisions relating to one's own belief systems and ideology count as fundamentally personal under section 7 has not yet arisen, but such a case may well be triggered by an ATA investigation. It is difficult to imagine how choices of this nature could be described as non-personal or unrelated to one's dignity and independence, given the existing language under this section.

While the section 7 right is theoretically subject to section 1, the Supreme Court has imposed a balancing exercise using the "principles of fundamental justice" mentioned in section 7 as an internal test for this right.¹³⁵ This test involves weighing the rights of the individual against those of the state,¹³⁶ and therefore section 1 is not often applied in cases where section 7 is invoked, since the internal test is considered a sufficiently rigorous balancing of interests. As will be seen, there are a few guideposts that indicate how this test might be applied to the section 7 privacy right in the context of the ATA. The most recent was in *Re Application under s. 83.28*,¹³⁷ which will be discussed in the final section of this paper.

3.3.3. Future Developments

The determinations the Supreme Court makes concerning the scope and content of the privacy right under section 7 will be key to dealing with a number of challenges raised by the anti-terrorism crime-fighting model. The first case to raise these issues in a related context is *Ruby v. Canada (Solicitor-General)*.¹³⁸

In *Ruby*, the appellant was seeking to view a file about himself that he believed was held by Canadian Security Intelligence Service (CSIS), the government intelligence agency, by using a provision of the *Privacy Act* that allows individuals access to personal information about themselves compiled by the state. CSIS refused to confirm or deny that such a file even existed, and invoked the Act's "national security" and "foreign confidences" exemptions as reasons why it should not be compelled to disclose any information to Ruby.

It should be noted that these exemptions have been elevated to *de facto* exclusions by the ATA. The *Ruby* case focuses on the older version of the *Privacy Act*, which section 104 of the ATA has since amended to allow the

134. *Ibid.* at para. 31.

135. *Re B.C. Motor Vehicle Act*, [1985] 2 S.C.R. 486, <<http://scc.lexum.umontreal.ca/en/1985/1985rcs2-486/1985rcs2-486.html>>.

136. *Rodriguez*, *supra* note 103 at pp. 622–623.

137. *Re Application under Section 83.28*, *supra* note 22.

138. *Ruby v. Canada (Solicitor-General)*, 2002 SCC 75, <<http://scc.lexum.umontreal.ca/en/2002/2002scc75/2002scc75.html>>, [2002] 4 S.C.R. 3 [*Ruby* cited to LexUM/S.C.R.].

Attorney-General to issue a certificate prohibiting the disclosure of designated information¹³⁹ to protect “international relations” and/or “national defence or security.”¹⁴⁰ This would both prevent the access provision in *Ruby* from being invoked, and halt any ongoing proceedings based upon it.¹⁴¹

The *Privacy Act* contains provisions mandating that where the government’s reliance on the exemptions at issue in *Ruby* is challenged, certain *ex parte* and *in camera* procedures are triggered for evaluating the Crown evidence. The *Ruby* appeal focused solely on the mandatory nature of these procedures, which prevented the appellant from gleaning any information about a possible file on himself. These arguments are particularly relevant to the ATA, since they could also be applied to the automatic cessation of access proceedings under the new ATA amendments.

The appellant argued that the imposed procedures affected the ability of an individual to access and ensure the accuracy and appropriateness of personal information held by the state,¹⁴² which in turn violated the privacy right to protection of one’s “biographical core of information” as laid out in *Mills*. While this “biographical core” was originally determined to be part of the section 8 privacy right in *Mills*, the appellants in *Ruby* raised it under the security head of section 7 as well. Arbour J, writing for the full court, did not raise any roadblocks to it being linked to section 7, declaring that “[t]he arguments presented under section 8 are entirely subsumed under section 7 and need not be addressed independently.”¹⁴³

Arbour J described the “biographical core” as including “information which tends to reveal intimate details of lifestyle and individual personal or political choices.”¹⁴⁴ She then stated that “there is an emerging view that the liberty interest in section 7 of the *Charter* protects an individual’s right to privacy.”¹⁴⁵ At this point in the judgment, Arbour J’s independent discussion of the section 7 right largely ceased.

She focused instead on the lower court’s views of the case, summarizing the Federal Court of Appeal’s statement that “in order for the right to informational privacy to have any substantive meaning it must be concerned both with the acquisition and the subsequent use of personal information.”¹⁴⁶ The appeal court’s position was, in Arbour J’s words, that “the right to privacy includes the ability to control the dissemination of personal information obtained by the government,”¹⁴⁷ and that this included a right of access to ensure the information was correct. Arbour J declined to endorse or discuss

139. *Privacy Act*, R.S.C. 1985, c. P-21, s. 70.1(1), <<http://laws.justice.gc.ca/en/P-21/95414.html>> [*Privacy Act*].

140. Austin, “Privacy a Casualty,” *supra* note 95 at p. 256.

141. *Privacy Act*, *supra* note 139 at s. 70.1(2).

142. *Ruby*, *supra* note 138 at para. 31.

143. *Ibid.* at para. 30.

144. *Ibid.* at para. 31.

145. *Ibid.* at para. 32.

146. *Ibid.* at para. 32.

147. *Ibid.* at para. 32.

these conclusions, stating that it was unnecessary to decide if section 7 was triggered.¹⁴⁸

Nonetheless, Arbour J then went on to analyse the case as if the section 7 right was indeed triggered, and concluded that: “[a]ssuming, for the purposes of this analysis, that the appellant has suffered a deprivation of his liberty or security of the person interest, that deprivation is not contrary to the principles of fundamental justice.”¹⁴⁹ She reiterated that these principles are “informed in part by the rules of natural justice and the concept of procedural fairness” and their application will vary according to the context of the case.¹⁵⁰ She found that they were not violated because of the very narrow nature of the provisions being challenged¹⁵¹ and their character as a very specific exception within the Act.¹⁵²

However, it certainly seems possible to interpret Arbour J’s decision as hinting that a broader section 7 privacy challenge against the legislation as a whole would have resulted in a slightly different analysis. The *Ruby* decision repeatedly reiterates the “narrow” application of Arbour J’s finding and emphasizes what the court was *not* being asked to decide:

The appellant is not challenging the right of a government institution, when faced with an access to information request under s. 12 of the Act, to refuse to disclose certain information on the basis of the exemptions enumerated in the Act. The appellant also does not challenge the right of the government under s. 16(2) to refuse to confirm or deny the existence of personal information when claiming an exemption. Within the context of a valid statutory scheme that permits the government to refuse to confirm or deny the existence of information (we must assume that it is valid since it is not challenged) and where the judicial review may conclude that the information was properly withheld and must therefore not be disclosed, it necessarily follows that a government institution must be able to make submissions *ex parte*.¹⁵³

It appears on the basis of *Ruby* that the “biographical core of information” is now incorporated into the section 7 privacy right and that untrammelled collection of such information without the subject being able to gain access to it or exercise any control may violate that right. This reading would suggest, amongst other possibilities, that there are ample grounds to challenge the newer version of the *Privacy Act* as amended by the ATA.

148. *Ibid.* at para. 33.

149. *Ibid.* at para. 33.

150. *Ibid.* at para. 39.

151. *Ibid.* at para. 51.

152. *Ibid.* at para. 46.

153. *Ibid.* at para. 41.

*

4. THE DEFINITION, THE RIGHT, AND THE PRINCIPLES OF FUNDAMENTAL JUSTICE

TO UNDERSTAND HOW THE PRIVACY RIGHT under section 7 would interact with the ATA definition of terrorism, it is instructive to trace how a hypothetical investigation of a suspected terrorist facilitator might proceed under the ATA's provisions, and how an ensuing *Charter* challenge could be brought. Let us posit that the subject of this investigation, Ali, came to Canada with his parents when he was a young boy. Ali has a childhood friend, Salim, who came to Canada as a young adult for educational purposes. Ali is a Canadian citizen, Salim is not. Unbeknownst to Ali, who was happy to renew ties with his old friend, Salim is involved with financing a terrorist organization located outside of Canada.

Ali and Salim spend quite a bit of time in each other's company. They go to the same mosque, attend functions at the homes of relatives of both, and socialize at the same local establishments, where they like to talk politics. Salim underplays some of his beliefs and does not disclose anything related to some of his financial or other affairs, in order to ensure Ali has no suspicion. Ali likes to exaggerate and explore ideas to their logical conclusion, so he often is the more heated of the two in their political discussions. Whenever stories about terrorists are on the news, Ali sometimes expresses the sentiment that he would never do anything violent himself and is upset by the way terrorists are acting in the name of his religion, but he can understand some of the motivations behind what the terrorists do.

Ali and Salim start up an organization to help immigrants and refugees settle into the community upon arrival in Canada. The organization receives government funding, and raises funds in the community so that it can provide loans to help new arrivals survive while they organize social assistance or start jobs, and to help small local businesses get off the ground. Salim, who is studying for an MBA, convinces Ali that he can handle the financial end of the enterprise and Ali just needs to co-sign various pieces of paperwork. Salim starts to use this organization to launder money for his group.

Salim believes that his secret cause must be furthered by any means necessary. So in addition to making sure Ali's signature is on all the relevant financial documents, he has also set up the records to make it appear as though he is acting at Ali's direction with the intent that Ali will be the fall guy for his operation if anyone catches on to what is occurring.

The Royal Canadian Mounted Police (RCMP) becomes suspicious of Salim based on information provided by CSIS, which has been hearing about Salim from its foreign intelligence sources. It places both Ali and Salim under observation. One of the officers involved in the investigation has had two complaints brought against him involving charges of racism in the past, one early in his career and one three years ago, but he was immediately cleared both times by an internal investigation. No independent investigation of the claims was ever conducted, and the officer's history has been affecting his ability to win the trust of minority groups he encounters in the course of his work. This officer

has just been transferred to anti-terrorism investigations, and this is his first direct exposure to the Muslim community.

This officer is soon able to piece together the financial chain that leads to Ali and Salim's immigrant and refugee assistance program, and now has a reasonable basis to believe that something is going on. Since he knows he must prove motivation as an element of a terrorist offence, he starts taking photographs of Ali and Salim going into their mosque, and sends a wired undercover officer to sit at the next table in their favourite café and listen to their conversations. His undercover counterpart reports back that he does not think the taped conversations reveal terrorist motivations, but the officer is not convinced.

So he gets an order to monitor the immigrant and refugee organization's email under the ATA-revised *Criminal Code*. Ali, who loves email, uses it to communicate with various friends. Salim, deliberately careful, uses the organization's email in a very limited fashion, sending no personal emails at all. Ali discusses some of his views about what he thinks might motivate terrorism in an email to a friend, and says again that he can "understand" it. Since he often talks with this friend and both know he does not support terrorism at all, he does not bother to reiterate his position against terrorism in the email.

The officer has been receiving intelligence about the imminent arrival of some terrorists in the country whose flight tickets and logistics are being arranged by Salim's organization. He decides it is time to move on the Canadian funding operation to prevent this, and places both Ali and Salim under preventive arrest without a warrant owing to the necessity, as he sees it, for speedy action under section 83.3(4). Based on the financial transaction evidence, the Solicitor-General declares Ali and Salim's immigration and refugee organization a "terrorist group" and puts it on the list of entities under section 83.05.

All of Ali's financial assets are immediately frozen, as are those of the organization, under section 83.14. Meanwhile, Ali is put into detention, awaiting the availability of a provincial court judge to hear the justification for his arrest. (A judge is supposed to be available within 24 hours but still has not been scheduled as of the next day, which is deemed permissible under section 83.3(6).)

The RCMP officer prepares charges of facilitation under section 83.19, when he hears that Salim has some information he is willing to offer. Salim, in the hopes of getting freed via a peace bond under section 83.3(8) and quietly leaving the country, tells the officer that he was only acting under Ali's instructions, and that the financial records will show this. The RCMP officer, who has already been able to seize the financial records of the organization after it became a listed entity, sits down and studies them. He adds on a charge of instructing to carry out activity for a terrorist group under section 83.21 against Ali as a result.

Ali's family, friends, and neighbours are shocked, and word spreads rapidly through the community. A family of newly arrived refugees who were due to receive a short-term emergency loan from Ali and Salim's organization the next day learn that they will not get the money they were relying on, and all of

Ali and Salim's clients start to be terrified that they will be deported for connections to "terrorists." Some wonder if they should just echo the authorities' negative views of Ali to demonstrate that they do not condone terrorist activities, while others simply plan to avoid all future contact with him.

Ali's family calls up Ali's workplace, a marketing company, to find out if his employer can help him retain legal counsel. The employer fires Ali instead, highly afraid of the impact on his clientele should they hear about the arrest. Ali manages to get duty counsel to represent him while his family hunts for another lawyer who will take on the case, as they start to argue amongst themselves about whether it is at all possible Ali had a secret life they did not know about.

By the time Ali gets in front of a judge, word has come in that the expected arrival of the possible terrorists from abroad may have been stopped, but this is irrelevant because both the facilitation and instruction offences still apply whether or not any terrorist act was actually carried out. The Crown has presented the evidence concerning Salim's connections *ex parte* to protect international relations and national security,¹⁵⁴ so Ali still does not know what is going on.

The RCMP officer presents the financial records to the judge, to show intent and act, in addition to Ali's email, taped conversations with Salim, and photographs of them entering a mosque as proof of motivation. Ali's case includes arguments that he believes Islam is a peaceful religion and that his political views have been taken out of the context of private discussions with intimates who know him to be non-violent. The judge decides that the officer had both reasonable belief of terrorism-related acts and reasonable suspicion of Ali's involvement, and has offered preliminary proof that the three elements of the offences can be met, which is all that is required under the ATA for the charge to proceed.

Ali's friends seek out a media outlet, hoping to spread word of his innocence, but the media concentrates instead on the sensational arrest, while adding only a line at the bottom of the article stating, "Ali's friends say they think he is innocent." By the next evening, Ali's picture is being flashed on local news screens as a "suspected terrorist." The judge is not convinced that the danger the organization's operation represents has been fully dealt with yet, and also decides that public confidence in the administration of justice will be affected if Ali is not kept in custody under section 83.3(7)(b)(C), so Ali continues to be detained pending trial.

Meanwhile, the RCMP officer is convinced that some of the immigrant and refugee clients of the "terrorist group" are likely to be involved as well and gets an investigative hearing under section 83.28 to compel them as witnesses, as well as more *Criminal Code* wiretapping orders to intercept their communications. Discussion about Ali, ranging from strong defence of his

154. ATA, s. 43 amended the *Canada Evidence Act*, R.S.C. 1985, c. C-5, <<http://laws.justice.gc.ca/en/C-5/16211.html>>, to allow the Attorney-General to present *ex parte* on these grounds at s. 38.11(2) of the *Criminal Evidence Act*, applied in conjunction with the provisions under s. 38.06 of the *Canada Evidence Act*.

innocence to wild speculation about him and his imaginary motives, is recorded. Some of the refugees whose loan accounts at the organization were used in Salim's financial dealings start to be preventively arrested as well.

The nature of the facilitation and instructing provisions, as well as the nature of the provisions governing listed entities, mean that it does not matter whether what Ali is supposed to have facilitated is clear, nor does it matter that no direct harm has occurred as a result. Since these provisions also state that the charge is applicable whether or not the accused knows that what he is facilitating is terrorism, Ali's denials of knowledge or ill-intent may not be convincing either. And while Ali's lawyer can try to argue that Ali's organization is not a terrorist group, the Solicitor-General does not have to provide proof beyond a reasonable doubt of why it is on the terrorist list, nor does he have to share the evidence with Ali.

An application can be made under section 83.05(6) to get a judicial hearing about whether the "terrorist group" designation is based on reasonable and probable grounds, but there is no requirement that the applicant be able to see the evidence, nor that the evidence be admissible under normal standards.¹⁵⁵ The Attorney-General has certified information about Ali and Salim under the *Privacy Act*, so Ali's likelihood of being able to discover, access, or use Salim's intelligence files to cast doubt on his "confessions" is low.

This puts Ali's lawyer in a position of having to defend his client's alleged religious and political views in court, and to possibly call a parade of witnesses to testify about what they consider to be Ali's deeply held beliefs, in order to counter evidence from taped gossip within the community, all evidence that would clearly be inadmissible in any other setting. The lawyer begins to look into a *Charter* challenge.

At this point, it should be noted that all three stages of the continuum of privacy have been pushed back as far as they can go in Ali's case—state actors have (incorrectly) decided what he is thinking and the nature of his personal views, using information that they gleaned from spying on his private activities, conversations, and correspondence, and have in the process disrupted and distorted his close relationships with family, friends, and clients whom he was trying to assist. He is being questioned about his innermost beliefs and motivations by police officers, lawyers, and judges.

The kind of personal information collected about Ali and others under the discretion given to state actors in the ATA clearly falls within the "biographical core of information" apparently protected under section 7 of the *Charter* since *Ruby*. Not only that, but these "intimate details of the lifestyle and individual personal or political choices"¹⁵⁶ are being used as a basis for Ali's alleged guilt, which could be considered a state invasion into the "irreducible sphere of personal autonomy wherein individuals may make inherently private choices free from state interference."¹⁵⁷ The preventive arrest of Ali on the basis of these details has also created a criminal "stigma" that would meet the

155. *Criminal Code*, *supra* note 1, s. 83.05(6.1).

156. *Ruby*, *supra* note 138 at para. 31.

157. *Godbout*, *supra* note 129 at para. 66.

Morgentaler and *Blencoe* description of “serious state-imposed psychological stress.”¹⁵⁸

There is a clear argument that the liberty and security heads of section 7 have been triggered on a number of fronts by privacy invasions which stem specifically from the motivational element in the ATA definition. It is the definition of “terrorist activity” that allows Ali’s beliefs to be monitored and allows the state to invade Ali’s sphere of autonomy by displacing the content of Ali’s beliefs with imputed beliefs of its own. Only the word “reasonable” stands between the arbitrary substitution of state beliefs for Ali’s, and it could well be argued that this is not enough protection to meet the “procedural fairness” requirements of the principles of fundamental justice.

Whether Ali’s lawyer chooses to make the section 7 argument under security, liberty, or both, the strength of Ali’s section 7 privacy rights will be determined by a balancing exercise against those principles. This involves a contextual weighing of the interests of the individual against the interests of the state,¹⁵⁹ as well as what is in accordance with the common law rules of procedural fairness.¹⁶⁰ Arbour J observed in *Ruby* that “[i]t is also necessary to consider the statutory framework within which natural justice is to operate.”¹⁶¹ This is of particular relevance in the case of Ali, since it is the ATA definition’s interactions with the other evidentiary rules and offences that could be so damaging to him.

In this situation, the state interest is national security and the need to keep Canadians safe by combating terrorist threats. This particular interest was discussed at length in *Suresh*,¹⁶² the same decision in which the Court provided the alternate terrorism definition still used for IRPA. Based on this definition, it decided that deporting a suspected terrorist to torture violated the principles of fundamental justice, observing that “states must find some other way of ensuring national security.”¹⁶³

However, the Court’s stance concerning the decisions of state actors on national security issues was generally deferential.¹⁶⁴ It stated that where terrorism is concerned, direct proof is not mandatory:

[...] to insist on direct proof of a specific threat to Canada as the test for “danger to the security of Canada” is to set the bar too high. There must be a real and serious possibility of adverse effect to Canada. But the threat need not be direct; rather it may be grounded in distant events that indirectly have a real possibility of harming Canadian security.¹⁶⁵

158. *Blencoe*, *supra* note 107 at paras. 56–57.

159. *Rodriguez*, *supra* note 103.

160. *Singh v. Minister of Employment and Immigration*, [1985] 1 S.C.R. 177, <<http://scc.lexum.umontreal.ca/en/1985/1985rcs1-177/1985rcs1-177.html>> at pp. 212–213.

161. *Ruby*, *supra* note 138 at para. 39.

162. *Suresh*, *supra* note 2.

163. *Ibid.* at paras. 75–76.

164. The *Suresh* decision was written by “the Court” as a whole rather than being attributed to an individual judge to emphasize its unanimity on this issue.

165. *Suresh*, *supra* note 2 at para. 88.

The Court then went on to define “serious” as: “grounded on objectively reasonable suspicion based on evidence and in the sense that the threatened harm must be substantial rather than negligible.”¹⁶⁶ The “reasonable suspicion” standard to be applied in cases related to terrorism is not a particularly strong guarantee of procedural fairness, but it does at least require that the suspicion be “objectively” reasonable, rather than consisting of the bare substitution of the state’s subjective beliefs about Ali’s views, based on what can only be circumstantial evidence, for his stated views.

As previously discussed, it is not clear that the motivational element of the ATA definition, which gives rise to the kind of evidence-gathering and imputation of beliefs used against Ali, is actually necessary in order to catch and convict terrorists. In addition to encouraging a breach of the privacy rights of both suspects and unrelated third parties, it could even give actual terrorists an “out” through their option to deny beliefs, with the judge then in the position of having to make a call on highly speculative evidence.

As with traditional criminal offences, and the American definition of terrorism, offenders could be tried on the basis of intent and act alone. It is true that the standards of proof in the ATA governing intent and act might need to be more carefully tailored if that were the case, but since any *Charter* challenge is likely to implicate the offences resting on the definition, as well as the definition itself, this could be remedied were the Court to decide in Ali’s favour. It is here that an observation of Sopinka J’s in *Rodriguez* becomes relevant:

Where the deprivation of the right in question does little or nothing to enhance the state’s interest (whatever it may be), it seems to me that a breach of fundamental justice will be made out, as the individual’s rights will have been deprived for no valid purpose.¹⁶⁷

This observation was much discussed in the case of *Malmo-Levine*,¹⁶⁸ by both the majority and dissenting justices. Gonthier and Binnie JJ noted that one of the differences between a section 7 and a section 1 analysis is that the onus to prove a violation of section 7 rests on the claimant.¹⁶⁹ This is the most difficult aspect of a section 7 challenge for Ali. Owing to the Court’s stated tendency to defer to the judgment of the government on matters relating to national security, and the general lack of information with which Ali is likely to be operating, it may be quite difficult for him to attack the ATA definition on the grounds that it does not serve the state anti-terror purpose as a practical matter.

However, Gonthier and Binnie JJ also stated in *Malmo-Levine* that an analysis of whether the means justify the ends, similar to that under section 1, can be made by a claimant using a standard of “gross disproportionality.”¹⁷⁰ Arbour J added in her dissent that “[t]he risk of harm to society occasioned by

166. *Ibid.* at para. 90.

167. *Rodriguez*, *supra* note 103 at p. 594.

168. *R. v. Malmo-Levine; R. v. Caine*, 2003 SCC 74, <<http://scc.lexum.umontreal.ca/en/2003/2003scc74/2003scc74.html>>, [2003] 3 S.C.R. 571 [*Malmo-Levine* cited to LexUM/S.C.R.].

169. *Ibid.* at para. 97.

170. *Ibid.* at para. 143.

the conduct must then be balanced against the costs imposed upon society by the prohibition of the conduct in question."¹⁷¹

The argument in Ali's favour would rest on the proposition that the state's ability to catch terrorists is not impaired at all, and is possibly enhanced, by the removal of the motivational component of the ATA definition. Ali could argue that terrorist harms to society are not caused by people's beliefs; they are caused by an intent to harm others and the resulting acts. Removal of political, religious and/or ideological motivation from the definition would not compromise the safety of Canadians; it would simply ensure that the costs of enforcing the laws against terrorism are not disproportionately borne by the segments of Canada's population that are currently associated with "suspect" beliefs. The risk of harm would remain the same, and the costs would be reduced.

LeBel J, in his dissent in *Malmo-Levine*, stated that a breach of fundamental justice "is made out if and when the response to a societal problem may overreach in such a way as to taint the particular legislative response with arbitrariness."¹⁷² In his opinion, the prohibition on marijuana possession breached section 7 because "[t]he fundamental liberty interest has been infringed by the adoption and implementation of a legislative response which is disproportionate to the societal problems at issue."¹⁷³ He specifically pointed to the imprisonment of users and the stigma created by their criminal record.

While a preventive arrest is not the same as a criminal record, the stigma associated with terrorism is deeply serious, and most of its effects are triggered by a preventive arrest or a listed entity declaration, not a final conviction. Terrorist "suspects" are subject to renewable terms of detention, "peace bonds" that set conditions on their release, and the seizure of personal assets and property, among other sanctions. Various agencies and authorities will keep extensive records on them and share information about them indefinitely. The resulting stigma is pervasive and lasting.

Deschamps J identified another problem related to proportionality in her *Malmo-Levine* dissent. She stated that the problem with the marijuana prohibition was the underlying lack of precision about where the harm was located: "[t]he harmful effects of marihuana use have already been discussed and are highly debatable. The harm caused by its prohibition, however, is clear and significant."¹⁷⁴ Similarly, the evidentiary value of following Ali to his mosque and interpreting his political conversations with friends is debatable, whereas the harm resulting to both Ali and his community from such practices is well within Ali's power to prove.

The nature of the interest being balanced against that of the state must also be kept in mind. Privacy protects people's right to their own subjective experience, and with it their liberty, autonomy, and integrity, both physical and psychological. As genetic, technological, and neuroscientific innovations offer

171. *Ibid.* at para. 250.

172. *Ibid.* at para. 279.

173. *Ibid.* at para. 280.

174. *Ibid.* at para. 299.

opportunities for surveillance and invasiveness of a kind never before dreamed of, there is a danger that privacy, as with all unprotected rights, will become a luxury to be purchased by those who are affluent or part of a more socially favoured group. It is imperative that effective safeguards against this eventuality be put in place at the dawn of the era of preventive crime-fighting, and that the principles of fundamental justice be understood to include them.

*

5. EXPANSION OF THE PRINCIPLES OF FUNDAMENTAL JUSTICE

THE TOUCHSTONES OF THE CANADIAN JURISPRUDENCE on privacy are of limited usefulness in tracing the boundaries of the principles of fundamental justice as they apply in this context. The “reasonable expectation of privacy” has been protected since *Hunter v. Southam Inc.*, but the full extent of what is “reasonable” has not yet been fully explored. One Supreme Court comment on its meaning was in a section 8 case, *R. v. Buhay*,¹⁷⁵ where Arbour J stated: “[t]he expectation does not have to be of the highest form of privacy to trigger the protection of section 8.”¹⁷⁶ According to Arbour J, a “high” expectation of privacy would apply to “one’s own body, home or office,” as well as “information which we choose to keep confidential—particularly that which is kept under lock and key.”¹⁷⁷

However, in the recent case of *Tessling*, Binnie J found that the privacy of the home extended no further than its external walls. While he acknowledged that the inhabitant of the home in this case did have a subjective expectation of privacy, he did not find that expectation objectively reasonable on the facts:

The information generated by FLIR imaging about the respondent does not touch on “a biographical core of personal information”, nor does it “ten[d] to reveal intimate details of [his] lifestyle”.... It shows that some of the activities in the house generate heat. That is not enough to get the respondent over the constitutional threshold.¹⁷⁸

This reasoning does not seem to take into account the traditional property concepts that Binnie J himself cited in the same decision, which would extend the protection of “home” to the entire property, not just the building. It also does not address the fact that the police were specifically conducting the warrantless surveillance to determine what was happening inside the home. Binnie J acknowledged in *Tessling* that American protection of the privacy right in the home is stronger than it is in Canadian jurisprudence, and quoted the statement of Dickson J (as he then was) in *Hunter v. Southam Inc.* that the section 8 right of privacy in Canada “protects people, not places.”¹⁷⁹ He also acknowledged that the oft-criticized “reasonable expectation of privacy”

175. *R. v. Buhay*, 2003 SCC 30, <<http://scc.lexum.umontreal.ca/en/2003/2003scc30/2003scc30.html>>, [2003] 1 S.C.R. 631 [*R. v. Buhay* cited to LexUM/S.C.R.].

176. *Ibid.* at para. 22.

177. *Ibid.* at para. 24.

178. *Tessling*, *supra* note 86 at para. 62.

179. *Hunter v. Southam*, *supra* note 79 at p. 159.

180. *Tessling*, *supra* note 86 at para. 43.

threshold is a “major battleground” in section 8 cases.¹⁸⁰

The procedural limits around a section 8 “reasonable expectation” are not necessarily automatically applicable to a section 7 right of privacy, but would certainly be relevant in informing procedural fairness considerations under the principles of fundamental justice. In *O'Connor*, L'Heureux-Dubé J explicitly drew on this section 8 language in her formulation of a test for balancing one section 7 right (privacy) against another (the accused's right to full answer and defence)¹⁸¹ in a case involving the production of therapeutic records for disclosure.¹⁸²

The Supreme Court had a recent opportunity in *Re Application under s. 83.28* to explicitly address the question of how privacy rights under section 7 are to be balanced against the principles of fundamental justice under the ATA. It gave a very incomplete answer. The case concerned a challenge to the investigative hearing procedure under the ATA legislation, with a related case addressing an order by a judge that the constitutional challenge to the provision be held *in camera*. The decisions for both cases were released in June 2004 on the same day. In the companion case, *Vancouver Sun (Re)*, Iacobucci and Arbour JJ referred to *Re Application under s. 83.28* as if they expected it to resolve a privacy question:

The Attorney General of British Columbia took the position that parts of the appeal, constituting stand-alone issues, could be held in public: the constitutionality of s. 83.28 of the Criminal Code, the role of the judge, and retrospective application of the provision. Mr. Bagri submitted that grounds of appeal relating to self-incrimination and privacy under section 7 of the Charter, judicial independence, and retrospectivity could be heard in public.¹⁸³

However, the decision handed down in *Re Application under s. 83.28* made no reference to privacy under section 7 at all. The constitutional question stated by McLachlin CJC was: “Does s. 83.28 of the *Criminal Code*, R.S.C. 1985, c. C-46, infringe s. 7 of the *Canadian Charter of Rights and Freedoms*?”¹⁸⁴ The analysis finding section 83.28 to be within section 7 limits was under a heading titled “The Right to Silence/The Right Against Self-Incrimination.” The court briefly acknowledged that the liberty interest was automatically engaged “at the moment of the compelled speech,”¹⁸⁵ but then analysed the impugned provision solely in relation to the principles of fundamental justice without any fuller discussion of the content of the liberty interest.

Iacobucci and Arbour JJ, again writing for the majority, stated that two

181. *O'Connor*, *supra* note 120 at para. 132.

182. While the compelled testimony of a religious confidant such as an imam under the ATA might be analogous to the production of therapeutic records, the *O'Connor* test will not be analyzed in-depth here, since someone accused of a terrorist offence is arguably likely to oppose such testimony rather than seek it, a situation that would be the reverse of the one the *O'Connor* test was designed to handle.

183. *Vancouver Sun (Re)*, 2004 SCC 43, <<http://scc.lexum.umontreal.ca/en/2004/2004scc43/2004scc43.html>>, [2004] 2 S.C.R. 332 at para. 19 (emphasis added).

184. *Re Application under Section 83.28*, *supra* note 22 at para. 26.

185. *Ibid.* at para. 67.

common law evidentiary principles must be applied to any implementation of section 83.28.¹⁸⁶ The first is use immunity, which prevents evidence given by a witness at an investigative hearing from being used against them in a subsequent proceeding, and the second is derivative use immunity, which prevents such evidence from being used as a basis for collecting other evidence against the witness. Iacobucci and Arbour JJ stated that this approach would provide procedural safeguards sufficient to render section 83.28 constitutional.¹⁸⁷

While the application of such evidentiary principles might protect the immigrant and refugee clients of Ali in our hypothetical scenario, it would do nothing for Ali himself, since the terrorist designation leading to his preventive arrest would be imposed by the Solicitor-General, outside the evidentiary protection of the judicial system. According to the reasoning in *Re Application under s. 83.28*, the traditional evidentiary principles would presumably have to be applied at Ali's trial, but one of the main problems with the motivation-based definition of terrorist intent is that proof of this element must rely on certain kinds of evidence that do not meet those traditional standards. By the time Ali reaches trial, the investigation, detention, and stigma arising from the prevention-based measures taken against him will have already done irreparable damage to his rights, even if he is exonerated.

The limited procedural protections acknowledged to be part of the principles of fundamental justice are no longer enough to truly protect privacy rights in any case. A comprehensive set of basic safeguards around the privacy of citizens in the face of new surveillance technologies would realistically have to entail wider protection. Elizabeth Paton-Simpson, quoting AJ McClurg, has observed that the right to privacy must mean more than just the right to "stay inside your house with the blinds closed."¹⁸⁸

Paton-Simpson has explored what might be considered the "outer limit" of the right, the reasonable expectation of privacy in public spaces. She noted that most people expect to be able to control such factors as whether the public place they are in is secluded, whether information about their movements is harmlessly dispersed amongst casual passers-by or systematically tracked, whether or not they are known to the people around them, whether social conventions about not intruding on strangers will be respected, whether or not a permanent record is being made of their actions, and whether or not there is someone watching them (a fact no longer easy to assess in light of technological surveillance). These factors might well be appropriate yardsticks with which to begin to measure the "irreducible sphere" of privacy accorded to each person by right in Canada.¹⁸⁹ The question is whether they will be subsumed into the

186. *Ibid.* at paras. 70–71.

187. Interestingly, it also extended these safeguards, usually applied in criminal cases, to cover deportation and extradition hearings under IRPA as well, *ibid.* at para. 79.

188. Elizabeth Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50:3 *University of Toronto Law Journal* 305 at p. 307.

189. *Ibid.* at pp. 321–332.

principles of fundamental justice.

When determining the basic tenets of the legal system thought to underlie the section 7 principles, it is important to remember that the legal protections necessary for fundamental justice change as society changes. In a pre-electronic environment, where the casual spying and insecurity of information that is now prevalent did not exist, there was no need for such an emphasis on the safeguarding of privacy rights. Now, however, technology is rapidly outpacing the law's ability to contain it within the rights framework, as Arthur J. Cockfield notes:

While anti-terrorism laws have been subject to explicit evaluation prior to implementation, less attention has been paid to the technological developments that surround these policy changes. Technology can introduce significant social changes while escaping the "pattern of deliberation and review" that governs legal change. The problem is that inattention to technological developments leads to an increased risk of unanticipated adverse social outcomes.¹⁹⁰

Perhaps aware of the need for a more flexible approach, the Supreme Court has developed a new test to identify the principles of fundamental justice, which it laid out in both *Malmo-Levine*¹⁹¹ and *Canadian Foundation for Children, Youth and the Law v. Canada (Attorney-General)*.¹⁹² The test has three components: the principle invoked must be a legal principle; there must be sufficient consensus that it is vital for our societal notion of justice; and it must be capable of being identified with precision and applied to situations in a manner that yields predictable results.¹⁹³

Some indications of the principles that may be floated as constituting "baseline" privacy protection for Canadians in a new era of technological invasiveness can be found in the rapidly proliferating privacy legislation. Canada has had the "quasi-constitutional"¹⁹⁴ *Privacy Act*¹⁹⁵ in place since 1985 to set rules for the collection, use, and disclosure of information about Canadians by the state. Legislation has been enacted federally for the collection, use, and disclosure of personal information in the private sector, which includes as a schedule the Canadian Standards Association's *Model Code for the Protection of Personal Information* (also frequently referred to as "Fair Information Practices" or FIP).¹⁹⁶ Those guidelines for the handling of personal information

190. Arthur J. Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance" 29:1 *Queen's Law Journal* 364 at pp. 380-381 (footnotes omitted).

191. *Malmo-Levine*, *supra* note 168.

192. *Canadian Foundation for Children, Youth and the Law v. Canada (Attorney General)*, 2004 SCC 4, <<http://scc.lexum.umontreal.ca/en/2004/2004scc4/2004scc4.html>>, [2004] 1 SCR 76 [*Canadian Foundation* cited to LexUM/S.C.R.].

193. *Ibid.* at para. 8.

194. *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, <<http://scc.lexum.umontreal.ca/en/2002/2002scc53/2002scc53.html>>, [2002] 2 S.C.R. 773 at para. 25 [*Lavigne* cited to LexUM/S.C.R.].

195. *Privacy Act*, *supra* note 139.

196. "Principles Set Out in the National Standard of Canada Entitled *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96," Schedule 1 of *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, <<http://laws.justice.gc.ca/en/P-8.6/93196.html>> [PIPEDA].

represent a different approach from the traditional constitutional analysis of privacy, since they are derived from consistent principles rather than individual expectations, reasonable or otherwise. These principles are: accountability, identification of purposes, consent, limitation of collection, limitation of use/disclosure/retention, accuracy, use of safeguards, openness, individual access, and enforcement of compliance.

How would these principles operate if they became principles of fundamental justice for the purposes of the privacy right? Their legal definition has been shaped in the separate sphere of private sector relations, but the concepts enunciated there, along with the *Privacy Act* jurisprudence, might be useful in understanding how these principles could govern just relations between the individual and the state.¹⁹⁷

The first issue of note is the point at which a possible privacy violation is considered to have occurred. As Lisa Austin has noted, the threshold for engaging the privacy statutes is lower than it currently is for the *Charter* privacy rights.¹⁹⁸ Both the *Privacy Act* and the federal private sector legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA),¹⁹⁹ govern only the use of “personal information,” rather than addressing a broader concept of privacy. However, both acts are triggered when the owner is “identifiable” by means of this personal information, rather than just at the point when that information is considered sufficiently sensitive. In other words, the moment at which a privacy violation begins under the legislation is formalized, rather than depending on a pre-balancing of factors. If certain information is of a type which could reveal your identity, it is automatically eligible for protection. This is closer to the “biographical core of information” element of *Charter* privacy than the “reasonable expectation of privacy” model.

Once the information is considered capable of establishing identity, its handling is then subject to the ten *Model Code* principles. Two of these, accountability and identification of purposes, of necessity imply the need for someone to acknowledge that information is being collected and to be responsible for it, a principle which is particularly relevant to the mass stealth surveillance which can be carried out with new technologies. These principles are related to three others—individual access, accuracy, and openness—which can only be upheld by giving people the ability to look at information about themselves and give feedback about whether or not it is correct. These are the principles underlying the arguments in *Ruby*.

The collection, use, and disclosure of information are limited to what is

197. Indeed, the blurring of the lines between the state and the private sector with regard to the handling and storage of personal information may make the distinction between these two spheres less relevant than has traditionally been the case. As federal Privacy Commissioner Jennifer Stoddart has noted, the passage of the *Public Safety Act* in March 2004 and its amendment to PIPEDA allowing private sector organizations to collect information without consent for the purpose of reporting possible threats to the government “effectively permits these organizations to act as agents of the state.” Privacy Commissioner of Canada, *Annual Report to Parliament 2003-2004* (Ottawa: Public Works and Government Services Canada, 2004), <http://www.privcom.gc.ca/information/ar/200304/200304_e.asp>.

198. Lisa Austin, Lecture at the University of Toronto, 24 March 2004.

199. PIPEDA, *supra* note 196.

“reasonable,” and the Privacy Commissioner of Canada has developed a test applicable to PIPEDA which contains echoes of a section 1 analysis. In addressing a complaint by a railway employee who objected to constant surveillance by security cameras at work, the Privacy Commissioner assessed reasonableness by means of four questions: is this information demonstrably necessary to meet a specific need? Is it likely to be effective in meeting that need? Is the loss of privacy proportional to the benefit gained? And is there a less invasive way of achieving the same end?²⁰⁰

The limitations on collection, use, and disclosure follow from this test, although the technological demands inherent in upholding these principles restrict their application in practice. Many organizations, including government departments and agencies, use database technology developed long before the *Model Code*, which does not always contain the controls necessary to effectively limit data-sharing and access authorization, nor the hacker-proof security features contemplated by the safeguards principle. The extent to which anyone can protect information is currently limited by the nature of the tools they use to handle it, and this is true of all technological innovations that are rapidly evolving without specifications to incorporate privacy requirements. As Lawrence Lessig has noted, North America’s “East Coast code” (law) and “West Coast code” (programming code) do not yet reflect each other’s imperatives.²⁰¹

Consent is a key principle in privacy law, although much of its implementation is still largely cosmetic. In the commercial context, PIPEDA allows “opt out” consent for collection, use, and disclosure of personal information in most circumstances. This means that consent is assumed unless someone takes the trouble to inform the organization otherwise. The more traditional form of “opt in” consent is used only with information that is considered particularly sensitive, such as medical and financial information.

Such practices are of concern because consent for an initial gathering of information does not always translate into control over what happens to it after it is collected, particularly when the state is the collector. In *Re Privacy Act*,²⁰² the Federal Court of Appeal found that information collected by the government can be shared among departments for varying purposes without consent or even notice under the statutory scheme. In this case, a woman illegally receiving Employment Insurance benefits while living outside the country was caught by a new Revenue Canada internal practice requiring customs officials to disclose information to the Canadian Employment Insurance Commission on who was crossing the border. Décaré JA stated:

The *Privacy Act* therefore clearly contemplates, and distinguishes between,

200. *Employee Objects to Company's Use of Digital Video Surveillance Cameras* (23 January 2003), Privacy Commissioner of Canada *PIPED Act Case Summary #114*, <http://privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp>.

201. Paper presented to *Internet and the Law: A Global Conversation*, conference, University of Ottawa, Canada, 1 October 2004; see also Lessig, “The Code is the Law” *Industry Standard* (9 April 1999), <<http://www.lessig.org/content/standard/0,1902,4165,00.html>>.

202. *Re Privacy Act*, [2000] 3 F.C. 82, <<http://decisions.fct-cf.gc.ca/fct/2000/a-121-99.shtml>>.

the collection of information, which can only be for purposes related to the activity of the institution ... and the disclosure of information, which, in most cases, is for purposes other than those for which it was collected and for purposes related to the activity of the requesting institution.²⁰³

The Supreme Court of Canada dismissed the appeal and explicitly endorsed the lower court's findings.²⁰⁴ It also dismissed the appeal in a related case, *Smith v. Canada (Attorney General)*,²⁰⁵ where the Federal Court of Appeal had found that the *Privacy Act* provisions permitting this practice did not violate section 8 of the *Charter*. The Court stated:

[...] the appellant cannot be said to have held a reasonable expectation of privacy in relation to the disclosed portion of the E-311 Customs Information which outweighed the Canada Unemployment Insurance Commission's interest in ensuring compliance.²⁰⁶

There is not much of substance to analyse in this brief text, but it does reveal a troubling tendency to view privacy as a procedural safeguard in and of itself, instead of a right that requires procedural safeguards to enforce it. One wonders if such an approach would have withstood the presentation of privacy arguments under section 7 of the *Charter*, in the style of the subsequent *Ruby* case, with the procedural analysis clearly separated from the substantive discussion of the right.

The last of the *Model Code* principles, enforcement, depends on the implementation of the others. Wherever the collection, use, or disclosure of data about people's lives without notice or consent is allowed, they are powerless to know what is happening and to enforce their privacy rights, and their ability to turn to the state is limited where agents of the state are the ones gathering the information.

It may now not only be useful but pressingly necessary to elevate these principles to a constitutional level, since their enforcement at the regulatory level has been somewhat diluted. The concerns that PIPEDA was meant to address have already been largely subordinated to the demands of the new predictive crime model. Both the ATA and the recent *Public Safety Act 2002* (which received Royal Assent in May 2004), have amended PIPEDA in ways that essentially pre-empt its provisions where law enforcement and security concerns are invoked. The ATA inserted a new section 4.1 into PIPEDA (and, as mentioned earlier, a new section 70 into the *Privacy Act*) that removed all right of access to information about oneself held by the government where it has been certified

203. *Ibid.* at para. 17.

204. *Privacy Act (Can.) (Re)*, 2001 SCC 89, <<http://scc.lexum.umontreal.ca/en/2001/2001scc89/2001scc89.html>>, [2001] 3 S.C.R. 905 [*Privacy Act (Can.) (Re)* cited to LexUM/S.C.R.].

205. *Smith v. Canada (Attorney-General)*, [2000] F.C.J. No. 174 (QL), <<http://decisions.fct-cf.gc.ca/en/2000/t-1296-97/t-1296-97.html>>.

206. *Smith v. Canada (Attorney-General)*, 2001 SCC 88, <<http://scc.lexum.umontreal.ca/en/2001/2001scc88/2001scc88.html>>, [2001] 3 S.C.R. 902 at para. 2 [*Smith v. Canada (Attorney-General)* (SCC) cited to LexUM/S.C.R.].

to pertain to national security. The *Public Safety Act* amended sections 7(1) and (2) of PIPEDA to allow collection of personal information without consent where it is "required by law"²⁰⁷ and extended the provisions allowing law enforcement disclosure to use and collection as well.

Lisa Austin has critiqued the ATA amendments to Canada's privacy legislation, describing the current constitutional language for balancing privacy and security concerns as "inadequate."²⁰⁸ She adds: "this raises a dilemma for anyone seeking to claim that the government's proposals are consistent with *Charter* values: they may be consistent with current *Charter* thinking but that thinking may be inadequate to deal with the challenges posed by the present context."²⁰⁹

This is precisely the problem. While the Supreme Court may soon be forced to articulate a full-fledged privacy right under section 7, it has not yet resolved the issue of how much privacy is consistent with the entitlement of Canadians to fundamental justice in their dealings with the state. Any determination it makes must be able to stand up against the day-to-day living conditions created by new technologies as they emerge.

Many would argue that even the *Model Code* principles do not provide an adequate roadmap for the new technological landscape. Tina Piper has proposed²¹⁰ that Canada adopt the "Canadian Charter of Privacy Rights," a stronger document based on a 1997 report by the House of Commons Standing Committee on Human Rights and Status of Persons with Disabilities and introduced twice as a Private Member's Bill. The proposed *Act to Guarantee the Human Right of Privacy*²¹¹ passed first reading in the Senate in 2000, and in the following session made it through another first reading and debate on a second reading in 2001, and then died on the Order paper.

Piper views the privacy protection under section 7 of the *Charter* to be too limited, and suggests that the privacy charter be adopted as a stand-alone enactment. She provides an excellent discussion of why it is growing increasingly necessary for Canada to have a more extensive definition of privacy than the legislation has so far provided, and her analysis is equally applicable to the jurisprudence. But the initiative to introduce the privacy charter preceded 9/11, then stalled in the Parliamentary session of that year and has not been re-introduced since. It is doubtful that the proposed enactment could succeed, let alone acquire the entrenched status and moral authority necessary to enforce it,

207. *Public Safety Act 2002*, S.C. 2004, c. 7, <<http://laws.justice.gc.ca/en/P-31.5/96121.html>>, ss. 98(1) and (2).

208. Austin, "Privacy a Casualty," *supra* note 95 at p. 262.

209. *Ibid.*

210. Tina Piper, "The Personal Information Protection and Electronic Documents Act: A Lost Opportunity to Democratize Canada's 'Technological Society'" (2000) 23:2 *Dalhousie Law Journal* 253.

211. Bill S-21, *An Act to guarantee the human right to privacy*, 2d Sess., 36th Parl., 1999-2000, <http://www.parl.gc.ca/36/2/parlbus/chambus/senate/bills/public/S-27/S-27_1/S-27_text-e.htm> and Bill S-21, *An Act to Guarantee the Human Right to Privacy*, 1st Sess., 37th Parl., 2001, <http://www.parl.gc.ca/37/1/parlbus/chambus/senate/bills/public/S-21/S-21_1/s-21toce.htm>.

in the current preventive crime-fighting context.

However, it is possible that the contents of the privacy charter would meet the newly enunciated test for inclusion in the principles of fundamental justice. Several versions of the document even included a limitation akin to section 1 of the *Charter*, which would be consonant with the practice of doing an internal balancing of section 7 without recourse to the *Oakes* test.

The text cited by Piper is from the original recommendations proposed by the Standing Committee, which did not make it into the version of the proposed privacy charter that was introduced in Parliament. However, this original Committee text is worth reproducing in full again here, since it contains a blueprint of privacy principles enunciated with much greater precision than in the *Model Code*, the proposed bills, or any other document so far prepared for a Canadian audience:

1. Fundamental Privacy Rights and Guarantees

1.1. Everyone is entitled to expect and enjoy:

- physical, bodily and psychological integrity and privacy;
- privacy of personal information;
- freedom from surveillance;
- privacy of personal communications;
- privacy of personal space.

1.2. Everyone is guaranteed that:

- these privacy rights will be respected by others adopting whatever protective measures are most appropriate to do so;
- violations of these privacy rights, unless justifiable according to the exceptions principle which follows, will be subject to proper redress.

2. Justification for Exceptions

Exceptions, permitting the rights and guarantees set out above to be infringed, will only be allowed if the interference with these rights and guarantees is reasonable and can be demonstrably justified in a free and democratic society.

3. General Obligations

3.1. The basic duties owed to others to ensure their privacy rights are adequately respected include:

- the duty to secure meaningful consent;
- the duty to take all the steps necessary to adequately respect others' privacy rights or, if their rights must be infringed, to interfere with privacy as little as possible;
- the duty to be accountable;
- the duty to be transparent;
- the duty to use and provide access to privacy enhancing technologies;
- the duty to build privacy protection features into technological designs.

4. Specific Rights Related to Personal Information

- Everyone is the rightful owner of their personal information, no matter where it is held, and this right is inalienable.
- Everyone is entitled to expect and enjoy anonymity, unless the need to identify individuals is reasonably justified.

5. Specific Obligations Related to Informational Privacy

5.1. The basic duties owed to others to ensure their informational privacy rights are adequately respected include, in addition to the general obligations set out above:

- the duty to hold sensitive personal information in trust;
- the duty to limit information collection to what is necessary and justifiable under the circumstances;
- the duty to identify the purpose for which personal information is collected;
- the duty to ensure the information collected is correct and of the highest quality;
- the duty to provide the people whose personal data is collected with access to that information and a means to review and, if they judge it necessary, to correct it;
- the duty to only use and disclose personal information for the purposes identified when meaningful consent was obtained;
- the duty to keep personal information only for as long as is necessary and justifiable;
- the duty not to disadvantage people because they elect to exercise their rights to privacy.²¹²

This is a list of legal duties and principles that are identified with precision, reflect a growing societal consensus, and can be applied in a predictable manner, as required by the *Malmo-Levine*²¹³/*Canadian Foundation*²¹⁴ test for the principles of fundamental justice. It will be difficult for the Supreme Court to avoid applying them if its *Charter* analyses of privacy are to maintain their relevance and substance in the face of the new powers bestowed by the information age.

★

6. CONCLUSION

ON 29 MARCH 2004, the first charges under the ATA were laid against Mohammad Momin Khawaja, a young software engineer. According to press

212. Sheila Finestone (Chair), "Privacy: Where Do We Draw the Line?" *3rd Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities*, April 1997, Appendix III, available at Office of the Privacy Commissioner of Canada, <www.privcom.gc.ca/information/02_06_03d_e.pdf>.

213. *Malmo-Levine*, *supra* note 168.

214. *Canadian Foundation*, *supra* note 192.

215. Roy MacGregor, "An Unreal Day Unfolds at the Norman Rockwell Look-alike House" *Globe and Mail* (31 March 2004) A2 [MacGregor, "Unreal Day"].

reports, the RCMP broke into the Khawaja family home with a battering ram²¹⁵ (even though Khawaja himself was arrested at work²¹⁶) and tied the hands of family members while they searched the house.²¹⁷ A university history assignment written by one of the suspect's brothers was confiscated.²¹⁸ Another brother, Qasim Khawaja, was quoted as saying that most of the eight hours of questioning that the family underwent was taken up with questions about political affiliations and "our personal views about events. What I thought about the Madrid bombing, stuff like that."²¹⁹ He called the charges against his brother a product of the RCMP's "vivid imagination."²²⁰

The charges against Khawaja may or may not prove well-founded in the long run, but in either case it is noteworthy that the RCMP apparently questioned his family exhaustively about their own political views. Given the preventive arrest provisions that might have been invoked under the circumstances, one might wonder about the extent to which the family's eventual release depended upon their answers. The scene surrounding Khawaja's arrest is a textbook example of the kind of privacy violation that is encouraged and facilitated by the ATA's definition of terrorism.

In June 2006, a new wave of seventeen terrorism arrests, including five suspects too young to be named, stunned the country. It remains to be seen how the courts will adjust to the new era of crime-fighting and how they will interpret the terrorism definition as the cases of Khawaja and the others start to be tried.²²¹ But as the information-gathering power of the state increases, the fledgling privacy right protected under section 7 has a profoundly important role to play, and its breach as a matter of sweeping investigative routine is not a matter to be taken lightly.

The right to privacy will be of paramount concern in the coming decades as the parameters for the use of invasive technologies are set up to protect the general populace from both the state and any other party that would misuse them. Meanwhile, terrorism investigators hope to use such technologies in as unobstructed and wide a manner as possible, and the ATA definition compounds this problem by providing them with legislative encouragement to inquire into areas of human motivation that were previously off-limits. These developments are on a collision course, and a re-conceptualized approach to privacy under section 7 may be the best, and perhaps only, means of resolution.

216. Colin Freeze & Kim Lunman, "RCMP Lay Terrorist Charges" *Globe and Mail* (31 March 2004) at p. A1.

217. Mary Gordon, "Foreign Affairs Worker Tied to Terror" *Toronto Star* (31 March 2004), <http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1080688213518&call_pageid=968332188492&col=968793972154> [Gordon, "Foreign Affairs"].

218. MacGregor, "Unreal Day," *supra* note 215.

219. Gordon, "Foreign Affairs," *supra* note 217.

220. *Ibid.*

221. Sasha Nagy, "Massive Terror Attack Averted: RCMP" *Globe and Mail* (3 June 2006), <http://www.theglobeandmail.com/servlet/story/RTGAM.20060603.warrants0603_3/BNStory/National/home>.

