Surfing the Surveillance Wave: Online Privacy, Freedom of Expression and the Threat of National Security

David M. Tortell*

This article traces the emergence of section 2(b) of the Canadian Charter of Rights and Freedoms *as a response to privacy breaches resulting from internet government surveillance. Just as significant privacy rights have been read into sections 7 and 8 of the* Charter*, the author argues that section 2(b) can likewise be viewed through a privacy lens, particularly in the online context. The author first examines the concept of privacy, addressing definitional problems and the ways in which privacy has been located in, and excluded from, the* Charter*. Next, he focuses on aspects of section 2(b): the chilling effects of surveillance, freedom of thought and the pinpointing by Canadian courts of connections between privacy and expression. The article concludes with a review of ongoing constitutional challenges which embrace a privacy-centric approach to section 2(b) in attacking state surveillance powers created by Canada's 2001 and 2015 anti-terrorism statutes.*

L'auteur retrace l'apparition de l'article 2(b) de la Charte canadienne des droits et libertés *comme une réaction aux atteintes à la vie privée résultant de la cybersurveillance gouvernementale. Tout comme les articles 7 et 8 de la* Charte *ont été interprétés comme incluant des droits de la protection des renseignements personnels importants, l'auteur soutient que l'article 2(b) peut également être considéré à travers le prisme de la vie privée, notamment dans un contexte en ligne. Il examine d'abord le concept de la vie privée, abordant des problèmes de définition et les façons dont la vie privée a été située dans (et exclue de) la* Charte*. Ensuite il se penche sur des aspects de l'article 2(b) : les effets effrayants de la surveillance, la liberté de pensée et la détermination par les tribunaux canadiens des liens entre la vie privée et l'expression. Cet article se termine par un examen des contestations constitutionnelles actuelles qui incluent une approche à l'article 2(b) axée sur la vie privée en attaquant les pouvoirs de surveillance étatiques créés par les lois antiterrorisme canadiennes de 2001 et 2015.*

* Counsel, Ontario Ministry of the Attorney General. The views expressed in this article are those of the author and do not purport to reflect the views of the Ministry of the Attorney General. The author in indebted to Professor Kent Roach for his comments on an earlier draft of this article.

1. Introduction

Everyone is preoccupied with surveillance nowadays, judging from the near ubiquity of academic and non-academic writing and popular sentiment that has been devoted to this topic in recent years, particularly after Edward Snowden's 2013 leak of classified National Security Agency documents. Everywhere one turns, one comes across warnings regarding the contemporary dangers of government intrusion (often with the help of a co-opted corporate sector), especially online, into the nether regions of our personal lives. According to Neil Richards, we now face a "digital privacy Armageddon,"[1] a political and technological tipping point threatening to tear down the private realm in ways unparalleled in our history. For Richards and others, "privacy is one of the most important questions facing us as a society,"[2] a state of affairs that has spawned a cottage industry of "how to" guides and other materials on anti-surveillance techniques. For instance, Laura Poitras, the documentary film-maker who along with Glenn Greenwald was instrumental in the release of the Snowden leaks, has published *Astro Noise: A Survival Guide for Living Under Total Surveillance*.[3] The Electronic Frontier Foundation, in a similar vein, has prepared "survival" resources, including "Ten Steps You Can Take Right Now Against Internet Surveillance"[4] and the web-based "Surveillance Self-Defense" project, billed by the Foundation as "Tips, Tools and How-tos for Safer Online Communication."[5]

This heightened concern is understandable, particularly in light of the Snowden revelations and ongoing debates regarding the legality of government incursions into internet privacy and the individual's right to be left alone. Roused by such state interference, and intent on upholding the multiple con-

1 Neil M Richards, "Four Privacy Myths" in Austin Sarat, ed, *A World Without Privacy: What Law Can and Should Do* (Cambridge: Cambridge University Press, 2015) 33 at 41.

2 *Ibid*.

3 (New York: Whitney Museum of Art, 2016). Edward Snowden is currently involved in developing an "introspection engine," a mobile telephone case designed to help users avoid surveillance. See Nathaniel Mott, "Edward Snowden Designs Phone Case to Show When Data is Being Monitored", *The Guardian* (22 July 2016), online: <https://www.theguardian.com/us-news/2016/jul/21/phone-case-privacy-data-monitor-bluetooth-wifi-snowden-introspection-engine>.

4 Danny O'Brien, "Ten Steps You Can Take Right Now Against Internet Surveillance" (25 October 2013), online: <https://www.eff.org/deeplinks/2013/10/ten-steps-against-surveillance>.

5 Online: <https://ssd.eff.org/en>. Such materials are also available in the Canadian context, as reflected in Laura Beeston's article "How to be Invisible: Designers Create Anti-Surveillance Products to Protect Privacy", *The Globe and Mail* (14 October 2015), online: <www.theglobeandmail.com/life/anti-surveillance-items-helping-people-go-off-the-grid/article26805195/>. See also Eric R Danton, "'The Shadow State Is Not Really a Shadow State': How Surveillance Anxiety Is Shaping Pop Culture", *Flavorwire* (23 February 2015), online: <flavorwire.com/506101/the-shadow-state-is-not-really-a-shadow-state-how-surveillance-anxiety-is-shaping-pop-culture>.

stitutional rights and interests breached in Canada and elsewhere through this stealth tracking of online activity, legal experts and non-specialists alike have initiated a "global push back against surveillance."[6] Focused on "law reform, including substantive statutory changes, the overturning of problematic constitutional doctrines, and improved oversight,"[7] this movement has sought to stem the tide of government snooping. More and more, the idea of privacy itself has been absorbed within this broader theme, so that as David Lyon writes "[h]owever privacy may have been conceived in times past, today it is tightly tied to avoiding surveillance."[8] For Lyon, who penned this insight over two decades ago, the electronic monitoring of our personal activities by government and corporate actors is the hallmark of the "surveillance society."[9] Once relegated to the province of conspiracy theorists and other "paranoid" types,[10] this Orwellian construct of the Big Brother state has returned with a vengeance and informs much of the current thinking about privacy and the web.[11]

In Canada, the flashpoint for such concern has been Bill C-51, the omnibus legislation which introduced new laws and amended existing statutes in ways that could be said to undermine privacy and other rights and interests. The centrepiece of this suite of legislative changes is the *Security of Canada Information Sharing Act* ("SCISA"),[12] which affords Parliament the ability to use and disseminate personal information without ever having to obtain consent from the targeted persons. Such sweeping powers, and the exceptionally broad definitions of "activity that undermines the security of Canada"[13] (section 2 of

6 Lisa M Austin, "Enough about Me: Why Privacy Is About Power, not Consent (or Harm)" in Sarat, *supra* note 1, 131 at 131. Austin adds: "If privacy is supposedly dead, it is a death whose report has been greatly exaggerated. The ongoing Snowden revelations have made us all acutely aware that the internet has become an infrastructure of surveillance" (*ibid*).

7 *Ibid*.

8 David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis, MN: University of Minnesota Press, 1994) at 180.

9 *Ibid* at 3.

10 Beeston recaps: "We've come a long way from the tinfoil hat, that traditional aluminum trademark of conspiracy theorists. These days, the idea that average citizens need protection from Orwellian-style surveillance seems more practical than paranoid": Beetston, *supra* note 5. In "Humanizing Cyberspace: Privacy, Freedom of Speech, and the Information Highway" (1995) 28 Human Rights Research & Education Bull 1 at 5, Valerie Steeves anticipates this development in conjuring "images of an Orwellian future where Big Brother watches from every television screen and computer monitor."

11 George Orwell, *1984* (London: Penguin Books, 1954). First published in 1949 by Secker & Warburg Ltd.

12 *Security of Canada Information Sharing Act*, SC 2015, c 20, s 2.

13 *Ibid*, s 2. In *Our Security, Our Rights: National Security Green Paper, 2016* at 27 [*Green Paper*], the Government of Canada justifies this broad SCISA definition on the basis that it "covers a broad range of national security-related activities" and is "intended to provide flexibility to accommodate new

SCISA) and "terrorism offences in general" (section 83.221(1) of the *Criminal Code*[14]), showcase just some of the serious flaws critics have identified in the *Anti-Terrorism Act, 2015*.[15] In response to this government offensive on privacy, Canadians continue to demand transparency and safeguards. As Michael Geist declares: "Rather than slowing down work on Canadian privacy and surveillance policy, recent events in Europe point to the urgent need to address the inadequacies of Canadian oversight."[16] Striking the same tone, Ronald Deibert remarks that "Canadians are long overdue for a serious discussion about the proper limits of powerful security agencies like [the Communications Security Establishment ("CSE')] in the era of Big Data," adding that "[w]ithin a few short years we have fundamentally transformed our communications environment, turning our digital lives inside out."[17]

One of the casualties of this assault on privacy has been freedom of expression. There exists a necessary connection between these rights, a "speech-privacy matrix" or "continuum"[18] in which privacy, especially in relation to anonymity, facilitates truly free, unrestrained speech and thought. With the introduction of SCISA and other anti-privacy initiatives, the impact is more wide-ranging than an attack on privacy as understood in the narrow sense of control over one's personal information. Beyond this type of injury, protected by section 8 (and, in certain scenarios, section 7) of the *Canadian Charter of Rights and Freedoms*,[19] government surveillance could also interfere with section 2(b) rights. While the use of section 2(b) of the *Charter* to resist privacy invasions has received little attention in scholarship and case law to date, this possibility is being tested in a 2015 application commenced in Ontario Superior Court by the Canadian Civil Liberties Association ("CCLA") and Canadian Journalists for Free Expression ("CJFE") and a pair of 2014 cases brought in Federal Court by the British Columbia Civil Liberties Association ("BCCLA"). These cases (and a prior effort by the CCLA to impugn Canadian Security

forms of threats that may arise." Online: <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx>.

14 *Criminal Code*, RSC 1985, c C-46, s 83.221(1).

15 *Anti-Terrorism Act, 2015*, SC 2015, c 20.

16 Michael Geist, "What Now? Privacy and Surveillance in Canada After the Paris Attacks", *Canadian Progressive* (7 December 2015), online: <www.canadianprogressiveworld.com/2015/12/07/michael-geist-what-now-privacy-and-surveillance-in-canada-after-the-paris-attacks/>.

17 Ronald Deibert, "Who Knows What Evils Lurk in the Shadows?" in Edward M Iacobucci & Stephen J Toope, eds, *After the Paris Attacks: Responses in Canada, Europe and Around the Globe* (Toronto: University of Toronto Press, 2015) 191 at 200 [*After the Paris Attacks*].

18 David M Tortell, "Two Tales of Two Rights: *R v Spencer* and the Bridging of Privacy and Free Speech" (2016) 36:2 NJCL 253 at 255, 270.

19 *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 [*Charter*].

Intelligence Service ("CSIS") privacy-invasive powers) hint at a further means of defending against the surveillance state, and trace the emerging relevance of this largely neglected dimension of section 2(b).

In what follows I will trace this use of section 2(b) as a tonic to privacy breaches stemming from state surveillance practices, within and beyond the limits of Bill C-51. Just as a privacy right has been read into sections 8 and (more narrowly) 7 of the *Charter*, I propose that section 2(b) is also triggered by invasive government interception, use and sharing of personal information, especially in the online context. I first consider the privacy right, focusing on the challenges of defining this right and the limited ways in which it has been read into section 2(b) and other *Charter* provisions. Next, I turn my attention to the section 2(b) guarantee itself, examining the continuity of speech and privacy, the chilling effects of surveillance and the impact of technology on freedom of thought. This paper closes with a review of the above-noted CCLA/CJFE and BCCLA litigation, in an attempt to highlight present day uses of this privacy-centric approach to section 2(b) in Canadian courtrooms. This analysis, which mines legal and non-legal sources and ranges across different historical settings, seeks to contribute to discussions regarding the nature and limits of freedom of expression. Expanding the parameters of section 2(b) to make room for a privacy component, I argue, only enhances the menu of possible constitutional tools with which to shore up privacy, thereby promoting transparency and oversight in our own surveillance society.

2. The (expanding) parameters of privacy

A significant challenge in writing about "privacy" is the lack of consensus as to what this term means, conceptually and in practice, in any given context. In the most general sense, privacy can be understood as an attempt to protect private information from the gaze of others. Upon further scrutiny, however, this broad definition quickly unravels. Among other issues, the distinction between public and private realms has been rendered more complex with the advent of social media and other web platforms that allow, and in some sense require, that we live our private experiences in public. This lack of conceptual clarity is routinely picked up on by scholars, and constitutes a meeting point for many amidst the swirl of competing theoretical perspectives.[20] Of course,

20 See, for instance, Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford: Oxford University Press, 2015) at 112; Lesley A Jacobs, Nachshon Goltz & Matthew McManus, *Privacy Rights in the Global Digital Economy: Legal Problems and Canadian Paths to Justice* (Toronto: Irwin Law, 2014) at 4; Daniel J Solove, "A Taxonomy of Privacy" (2006) 154:3 U Pa L Rev 477 at 479; Mark Tunick, *Balancing Privacy and Free Speech: Unwanted Attention in the Age of*

this lack of clarity has not been lost on the Supreme Court of Canada. In *Dagg v Canada (Minister of Finance)*, Cory J. related that "[p]rivacy is a broad and somewhat evanescent concept."[21] Several years later Binnie J., in *R v Tessling*, concluded that "[p]rivacy is a protean concept,"[22] while Deschamps J. in *R v Gomboc* allowed that "privacy is a varied and wide-ranging concept."[23] Most recently, in *R v Spencer*, Cromwell J. advised: "Scholars have noted the theoretical disarray of the subject and the lack of consensus apparent about its nature and limits."[24]

While this definitional quagmire significantly confuses the issue at hand, it also has its benefits, especially in Canada and other jurisdictions that have not formally adopted a stand-alone constitutional right to privacy. This conceptual fluidity, while admittedly problematic, could nonetheless prove in situations where one needs the privacy construct to serve a number of different functions.[25] In the Canadian context, a flexible approach has allowed for the identification of privacy themes across distinct issues and scenarios. Thus, this concept is as much at home in debates over the right to make personal life decisions without state interference as it is in search and seizure lawsuits. Such malleability is a good thing, and provides a fuller canvas onto which to project existing and future possibilities for judicial expansions of privacy protections

Social Media, (New York: Routledge, 2015) at 24; Gus Hosein, "Privacy as freedom" in Rikke Frank Jørgensen, ed, *Human Rights in the Global Information Society* (Cambridge, MA: MIT Press, 2006) 121 at 122-24.

21 *Dagg v Canada (Minister of Finance),* [1997] 2 SCR 403 at para 67, 148 DLR (4th) 385 [*Dagg*]. In this decision, which focused on the definition of "personal information" at section 3 of the *Privacy Act*, the Court concluded that details regarding the number of hours worked by an employee fell within the section 3(j) exemption (information relating "to the position or functions of the individual") and could thus be disclosed.

22 *R v Tessling*, 2004 SCC 67 at para 25, [2004] 3 SCR 432 [*Tessling*]. Addressing the legality of Forward Looking Infra-Red ("FLIR") heat detecting technology, the Court found in this judgment that the defendant (whose marijuana grow operation had been detected through FLIR imaging) did not have a reasonable expectation of privacy in "[e]xternal patterns of heat distribution on the external surfaces of a house" (at para 63).

23 *R v Gomboc*, 2010 SCC 55 at para 19, [2010] 3 SCR 211. Building on *Tessling*, the Court held in this case that the use of a digital recording ammeter to detect electricity patterns consistent with a grow-op did not violate section 8 because the defendant did not have a reasonable expectation of privacy in such information.

24 *R v Spencer*, 2014 SCC 43 at para 35, [2014] 2 SCR 212 [*Spencer*]. In this case the Court ruled that the police's warrantless collection of subscriber information from an Internet Service Provider (ISP) constituted an unreasonable search and violated section 8 of the *Charter*.

25 One could argue that such fluidity is central to the *Privacy Act*, RSC 1985 c P-21, which at section 3 sets out a very broad definition of personal information that consequently blurs the limits and function of this legislation.

north of the forty-ninth parallel.[26] This is directly relevant to the application of section 2(b) in this context, and affords champions of this vision of free speech a stronger basis for reading privacy interests into section 2(b) than might otherwise be available were the contours of the *Charter* privacy landscape more firmly set in stone.

There is no stand-alone constitutional right to privacy in Canada, although things nearly turned out differently in the lead up to the 1982 launch of the *Charter*.[27] Despite this fact, constitutional protection of privacy interests has nevertheless made significant inroads over the last several decades. This is due in no small part to Justice La Forest, a well-known privacy booster who asserted in *R v Dyment* that privacy is "worthy of constitutional protection" and sits "at the heart of liberty in a modern state."[28] Abella and Cromwell JJ. concurred in *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*: "As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as 'quasi-constitutional' because of the fundamental role privacy plays in the preservation of a free and democratic society."[29] Such an approach to privacy,

26 As Lillian R BeVier writes in "Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection" (1995) 4:2 Wm & Mary Bill Rts J 455 at 458: "Privacy is a chameleon-like word, used … connotatively to generate goodwill on behalf of whatever interest is being asserted in its name."

27 On 20 January 1981, Jake Epp, a Progressive Conservative member of the Special Joint Committee of the Senate and of the House of Commons on the Constitution of Canada ("Committee") tasked with finalizing the contents of the proposed *Charter*, urged the Committee to adopt a stand-alone privacy right. Specifically, Epp moved (with support from the New Democrats) that "Clause 2" of the draft *Charter*, which dealt with "fundamental freedoms" be expanded to include a fifth section: section 2(e), guaranteeing "freedom from unreasonable interference with privacy, family, home, correspondence, and enjoyment of property." *Minutes of Proceedings and Evidence of the Special Joint Committee of the Senate and of the House of Commons on the Constitution of Canada*, 32nd Parl, 1st Sess, No 41 (21 January 1981) at 97 [*Minutes of Proceedings and Evidence*]. This proposal was defeated on January 22 by a mere four votes, as recounted in the Committee records: "it was negatived on the following show of hands: YEAS: 10; NAYS: 14": *ibid*, No 43 at 7. Following the voting down of section 2(e) Parliamentarians attacked this result in the House of Commons and continued to underscore the need for privacy protection. On January 29 Svend Robinson, a New Democrat, channelled Orwell in invoking "Big Brother" and admonishing that "as we approach that famous year of 1984 … we must ensure that the government does not have sweeping and arbitrary powers to intrude into the private lives of Canadians." *House of Commons Debates*, 32nd Parl, 1st Sess, No 6 (29 January 1981) at 6696. That same day Perrin Beatty, a Progressive Conservative, complained that while the "current government has endlessly argued that a complete and fundamental bill of rights ought to be included in any constitutional amendments … shockingly, one of the most basic of human rights has been left out of the government's charter of rights, and that is the right to privacy" (*ibid* at 6704).

28 *R v Dyment*, [1988] 2 SCR 417 at 427-28, 55 DLR (4th) 503.

29 A*lberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19, [2013] 3 SCR 733.

which Alysia Davies describes as an "overlooked *Charter* right,"[30] is viewed by Lesley A. Jacobs as "hermeneutic rights to privacy" which, although they "may not receive explicit recognition in the *Constitution Act, 1982*, [are] closely tied to existing constitutional rights and values."[31] International commentators have likewise taken notice of this homegrown "quasi-constitutional" model. As reported in a United Nations survey on online privacy and free speech, "many countries include a right to privacy in their constitutions, provide for it in specific laws or have had the courts recognize implicit constitutional rights to privacy, as they do in Canada."[32]

The original locus for this "implicit constitutional right" was section 8 of the *Charter*, a development in the law first charted in *Hunter v Southam*, in which, as summarized thirty years later by Binnie J. in *Tessling*, "the Court early on established a purposive approach to s. 8 in which privacy became the dominant organizing principle."[33] This use of section 8 as a vehicle for privacy cannot have come as much of a surprise in 1984, when *Hunter v Southam* was decided, given section 8's focus on search and seizure and the connection of such violations to the private sphere. Indeed, at least one member of the Parliamentary committee tasked in the early 1980s with drafting the *Charter* anticipated this application of section 8 to privacy rights,[34] and subsequent decisions of the Supreme Court of Canada and other courts have followed suit. Many of the foundational "privacy" judgments are rooted in section 8. This includes *Spencer*, which has propelled the jurisprudence into the twenty-first century through its attention to online activity and the role of internet service providers in disclosing personal subscriber information.[35] If one were forced to identify a part of the *Charter* most closely associated with privacy, section 8 would be it. It is important to remember, however, that although this *Charter* provision may constitute the most usual suspect in this regard, it has not cornered the market by any means.

30 Alysia Davies, "Invading the Mind: The Right to Privacy and the Definition of Terrorism in Canada" (2006) 3 U Ottawa L & Technology J 249 at 261.

31 Jacobs et al, *supra* note 20 at 23.

32 UNESCO, *Global Survey on Internet Privacy and Freedom of Expression* (2012) at 10-11, online: <unesdoc.unesco.org/images/0021/002182/218273e.pdf>.

33 *Tessling*, *supra* note 22 at para 19.

34 As noted by Liberal Member of Parliament Jean Lapierre on 22 January 1981: "I think that the concerns of [the Progressive Conservatives] relating to privacy, family, home and correspondence are guaranteed by Section 8 which offers a fairly wide array of protections.": *Minutes of Proceedings and Evidence*, *supra* note 27, No 43 at 58.

35 *Spencer*, *supra* note 24 at para 5.

Perhaps as a function of the "evanescent" or "protean" nature of privacy,[36] the Supreme Court of Canada has also read a privacy component into section 7 of the *Charter*. The evolution of section 7 in this regard is of particular interest since its protection of "life, liberty and security of the person," unlike section 8's emphasis on search and seizure, does not seem immediately connected to privacy. With respect to section 7, any such link is less straightforward and requires more conceptual legwork. For one thing, the phrase "life, liberty and security of the person" does not suggest the public-private divide to the same extent as "unreasonable search and seizure." It may have been for this reason that Dickson C.J.C., in his 1988 ruling in *R v Morgentaler*, declined to interpret section 7 within a privacy framework.[37] Justice Wilson, writing in this same judgment, took a different view, underlining that "an aspect of the respect for human dignity on which the *Charter* is founded is the right to make fundamental personal decisions without interference from the state. This right is a critical component of the right to liberty."[38] Her opinion has since been affirmed on a number of occasions, thus allowing section 7 to join section 8 as one of the *Charter* rights identified by the Supreme Court of Canada as protecting privacy interests. As stated by L'Heureux-Dubé in *R v O'Connor*, "This Court has on many occasions recognized the great value of privacy in our society" and "has expressed sympathy for the proposition that s. 7 of the *Charter* includes a right to privacy."[39]

In reviewing the ways in which privacy has been read into sections 7 and 8, the elastic nature of this interpretative process becomes clear, as does the fact that a privacy quotient need not be limited to these two *Charter* provisions. Put differently, given the absence of any dedicated privacy right and the flexibility of this concept, there is no reason why the hunt for privacy protection should end with sections 7 and 8. Daphne Gilbert adopts this position, maintaining that "the positioning of privacy in the Legal Rights section alone neglects privacy's relevance to other *Charter* guarantees."[40] Making the case

36 *Dagg*, *supra* note 21 at para 67; *Tessling*, *supra* note 22 at para 25.

37 *R v Morgentaler*, [1988] 1 SCR 30 at 51, 44 DLR (4th) 385 [*Morgentaler*].

38 *Ibid* at 166.

39 *R v O'Connor*, [1995] 4 SCR 411 at para 110, 130 DLR (4th) 235. The Supreme Court of Canada has also recognized the possibility of incorporating a privacy element into s 7 in other cases, including *R v Beare; R v Higgins*, [1988] 2 SCR 387 at 412, 55 DLR (4th) 481; *Edmonton Journal v Alberta (Attorney General)*, [1989] 2 SCR 1326 at 1376-1377, 64 DLR (4th) 577; *Dagg*, *supra* note 21 at para 66; *AM v Ryan*, [1997] 1 SCR 157 at para 79, 143 DLR (4th) 1; *Godbout v Longueuil (City of)*, [1997] 3 SCR 844 at paras 65-66, 152 DLR (4th) 577 and *Ruby v Canada (Solicitor General)*, 2002 SCC 75 at para 32, [2002] 4 SCR 3.

40 Daphne Gilbert, "Privacy's Second Home: Building a New Home for Privacy Under Section 15 of the Charter" in Ian Kerr, Valerie Steeves & Carole Lucock, eds, *Lessons from the Identity Trail:*

that privacy rights should also be located in section 15, she posits that "understanding privacy as an equality issue could present more expansive possibilities for safeguarding a range of different kinds of privacy interests, over and above those protected"[41] by sections 7 and 8. To stop there, she proposes, creates an "impoverished interpretation of what privacy could offer to human rights protections in Canada"[42] and an "incomplete and inadequate vision of a constitutional privacy interest."[43] For her, "finding a home" for privacy outside the parameters of sections 7 and 8 "opens new possibilities for expanding its constitutional protection and its utility as a tool in advancing other Charter rights."[44] Turning now to freedom of expression, I take up this argument on behalf of section 2(b), showing how it too can serve the interests of protecting privacy.

3. The freedom of expression-privacy connection

As I have written elsewhere,[45] there is a natural connection between freedom of expression and privacy that makes section 2(b) ripe for inclusion in that collection of *Charter* rights isolated to date as privacy-friendly. Just as sections 7 or 8 (or 15, as per Gilbert) can be viewed through the privacy lens, so too could section 2(b) be read in this way, particularly since the utility of privacy as a vehicle for free speech has been recognized by the Supreme Court of Canada in *Spencer*. If it was not sufficiently evident beforehand, Justice Cromwell's ruling, beyond finding a reasonable expectation of privacy in personal online subscriber information, establishes a constitutional link between privacy and speech. While the role of anonymity in fostering expression had previously been flagged in several judgments concerned with defamation in cyberspace, *Spencer* was the first substantive foray by the Supreme Court of Canada into such issues, especially vis-à-vis internet expression. Citing the work of A. F. Westin, Cromwell J. noted that "[a]nonymity permits individuals to act in public places but to preserve freedom from identification and surveillance,"[46] a real-

Anonymity, Privacy and Identity in a Networked Society (Oxford: Oxford University Press, 2009) 139 at 139.

41 *Ibid* at 145.

42 *Ibid* at 139.

43 *Ibid* at 144. Graham Mayeda, in "My Neighbour's Kid Just Bought a Drone … New Paradigms for Privacy Law in Canada" (2015) 35 NJCL 59 at 60, 83, similarly speaks of "emerging paradigms of privacy," arguing that "we need a more flexible legal notion of privacy" and that the "law must allow law-makers and judges more flexibility to recognize a new dimension of privacy."

44 Gilbert, *supra* note 40 at 139.

45 *Supra* note 18.

46 *Spencer*, *supra* note 24 at para 43. From the federal government perspective, *Spencer* is problematic in limiting access to certain types of information in a law enforcement context (*Green Paper*, *supra* note 13 at 63). The Privacy Commissioner of Canada has expressed a more positive view of *Spencer*,

ity of particular importance "in the context of Internet usage."[47] In this context, Cromwell J. singled out that "form of anonymity" critical to the author "who wants to present ideas publicly but does not want to be identified," which is one of the "defining characteristics of some types of Internet communication."[48]

Although *Spencer* may be the most significant Supreme Court of Canada decision to date dealing with the intersection of expression and privacy, it is not the first time that the Court has taken notice of the complementarity of these two fundamental interests. A review of the case law establishes that the Court has on a number of earlier occasions signalled the possibility of such a mash-up of constitutional principles. In C*anada (Human Rights Commission) v Taylor*, Dickson C.J.C., contrasting the extent and nature of hate speech protection in section 319(2) of the *Criminal Code* (which does not apply to private communications) with that in section 13(1) of the *Canadian Human Rights Act* (which does), opined that the "connection between s. 2(b) and privacy is thus not to be rashly dismissed."[49] The following decade, Chief Justice McLachlin underscored this link in *R v Sharpe* when she defined privacy not merely in terms of sections 7 and 8 but also in relation to section 2(b): "Privacy, while not expressly protected by the *Charter*, is an important value underlying the s. 8 guarantees against unreasonable search and seizure and the s. 7 liberty guarantee… . [It] may also enhance freedom of expression claims under s. 2(b) of the *Charter*, for example in the case of hate literature."[50] Taken together, these three decisions, rendered in 1990, 2001 and 2014, reflect the Court's ongoing pairing of these rights over many years.

Aside from the Supreme Court of Canada, other courts have traced the various ways in which privacy and speech interact. In the defamation context, leading cases like *Warman v Wilkins-Fournier*[51] and *King v Power*,[52] rendered by the Ontario Divisional Court and the Newfoundland and Labrador Superior Court respectively, have weighed the impact of anonymity on reputation and online expression. The Alberta Court of Queen's Bench, in *Harper v Canada*

finding that "impartial oversight in the form of judicial authorization is critical before sensitive personal information may be turned over to the State." *2015-2016 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act: Time to Modernize 20th Century Tools* (September 2016) at 23-24, online: <https://www.priv.gc.ca/media/4516/ar_201516_eng.pdf>.

47 *Spencer*, *supra* note 24 at para 45.

48 *Ibid*.

49 C*anada (Human Rights Commission) v Taylor,* [1990] 3 SCR 892 at 936, 75 DLR (4th) 577 [*Taylor*].

50 *R v Sharpe*, 2001 SCC 2 at para 26, [2001] 1 SCR 45 [*Sharpe* (SCC)].

51 *Warman v Wilkins-Fournier*, 2010 ONSC 2126, 100 OR (3d) 648.

52 *King v Power*, 2015 NLTD(G) 32, 374 Nfld & PEIR 285.

(Attorney General) — a challenge brought by Stephen Harper (then on hiatus from federal politics) to third party spending and advertising provisions of the *Canada Elections Act* — likewise points out the continuity of these rights. As Cairns J. recaps, pointing to *Sharpe* and *Taylor*: "There are cases which have found a connection between freedom of expression and privacy… . The jurisprudence is clear that privacy values can enhance or strengthen a claim under s. 2(b) of the *Charter*."[53] In the lower court *Sharpe* decision, similarly, Shaw J. of the British Columbia Supreme Court confirmed (again relying on *Taylor*) that the "case law on freedom of expression reflects the *Charter*'s concern for the right of privacy."[54] Even in the pre-*Charter* period, courts were alert to this feature of free speech. Berger J., commenting in *R v Bengert (No. 8)* in 1979, struck a decidedly modern note: "With the advance of technology, the possibilities for the infringement of privacy have proliferated… . [T]he right of privacy … is essential to freedom of thought and freedom of speech."[55]

These decisions signal an emerging view of the mutually enhancing relationship between expression and privacy, most recently articulated by Cromwell J. in *Spencer*. To be sure, these interests have frequently been characterized, by commentators and courts, as being opposed in interest, a long-championed notion of speech (and freedom of the press in particular) versus the private sphere crystallized in multiple Supreme Court of Canada judgments and the famous Warren and Brandeis article "The Right to Privacy."[56] That said, rulings like the ones just reviewed present the other side of the coin: the possibility of harnessing privacy as a vehicle for expressive freedom. This body of case law, touching on different topics across criminal and civil proceedings, tracks the expansion of section 2(b) along lines similar to those evidenced with respect to sections 7 and 8 of the *Charter*. Just as courts have read a privacy component into these two provisions, such jurisprudence telegraphs that "[i]nstead of being conflicting values, privacy and speech can instead be mutually supportive."[57] It seems reasonable to suggest, therefore, that section 2(b) has also come to provide a "new home" for this right, as Gilbert might put it,[58] given that this connection has been pinpointed by the Supreme Court of Canada and lower courts across the country.

53 *Harper v Canada (Attorney General)*, 2001 ABQB 558 at paras 184-85, 295 AR 1.
54 *R v Sharpe* (1999), 169 DLR (4th) 536 at para 44, 1999 CanLII 6380 (BCSC).
55 *R v Bengert, Robertson (No 8)*, 15 CR (3d) 37, 1979 CanLII 525 at para 5.
56 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4:5 Harv L Rev 193.
57 Richards, *supra* note 20 at 95.
58 Gilbert, *supra* note 40 at 139.

Reading section 2(b) as encompassing protection against privacy violations also makes sense, separate and apart from the foregoing judgments, in terms of broader principles of statutory interpretation regularly applied to this *Charter* provision. It is trite law that section 2(b) is intended to be understood and applied in an expansive manner. This idea found early expression in *Irwin Toy Ltd. v Québec (Attorney General)*, where the Supreme Court of Canada established that the "content of expression can be conveyed through an infinite variety of forms of expression" and accordingly called for a "broad, inclusive approach to the protected sphere of free expression."[59] In *Baier v Alberta*, LeBel J. reiterated this point, saying that "the Court has traditionally defined freedom of expression in broad terms."[60] Quoting an earlier Supreme Court of Canada decision, he continued that the "Court favours a very broad interpretation of freedom of expression in order to extend the guarantee under the Canadian *Charter* to as many expressive activities as possible."[61] McLachlin C.J.C., in *Sharpe*, provided context for such breadth by stressing the singular function played by section 2(b), depicted by her as being "[a]mong the most fundamental rights possessed by Canadians," a guarantee which "makes possible our liberty, our creativity and our democracy."[62]

Following in the footsteps of the "life, liberty and security of the person" makeover, section 2(b) would thus appear to be taking its place alongside sections 7 and 8 as a constitutional device for protecting Canadians against state-sponsored privacy violations. Evincing the "living tree" nature of our constitution,[63] this ongoing evolution of section 2(b) should provide comfort to those concerned over the growing technological (and, in some cases, ideological) reach of government into our private lives. As the spectre of surveillance grows, particularly online, and professional critics and regular citizens become more alert to this reality, it makes sense that this dimension of section 2(b) would come into greater focus. Of course, the privacy protections afforded by the "freedom of thought, belief, opinion and expression" guarantee will prove more apposite in some circumstances than in others. And while it is likely that any such use of section 2(b) will overlap with other *Charter* provisions (most

59 *Irwin Toy Ltd v Quebec (Attorney General)*, [1989] 1 SCR 927 at 969-70, 58 DLR (4th) 577.

60 *Baier v Alberta*, 2007 SCC 31 at para 90, [2007] 2 SCR 673.

61 *Ibid* at para 91, quoting *Libman v Quebec (Attorney General)*, [1997] 3 SCR 569 at para 31, 151 DLR (4th) 385. See also Peter W Hogg, *Constitutional Law of Canada*, 5th ed, vol 2 (Scarborough, ON: Carswell, 2007) (loose-leaf 2014 supplement) at Part 43:9-10; Robert J Sharpe and Kent Roach, *The Charter of Rights and Freedoms*, 5th ed (Toronto, Irwin Law, 2013) at 157.

62 *Sharpe* (SCC), *supra* note 50 at para 21.

63 *Edwards v Attorney-General for Canada* (1929), [1930] AC 124 at 136, [1930] 1 DLR 98 (Lord Sankey).

likely section 8), challenging state action on multiple grounds is a common litigation strategy. In the end, there is little downside in adding free speech to the constitutional privacy mix, especially given the potential contemporary threats to our web-based information security.

4. Grave new world of online surveillance

The pathways of the internet have had an indisputably positive impact on the well-being of persons worldwide, an innovation as paradigm shifting, arguably, as the introduction of the printing press in fifteenth century Europe. Canadian courts understand this reality, taking notice in their decisions of this "communications revolution" and its "heralding [of] a new and global age of free speech and democracy."[64] Justice Abella, speaking for the majority of the Supreme Court of Canada in *Crookes v Newton*, which probed the legal responsibility of authors for defamatory hyperlinks included in their work, observed that the "Internet's capacity to disseminate information has been described by this Court as 'one of the great innovations of the information age.'"[65] This comes as no surprise, certainly, as we take for granted (at least in wealthy first world communities) that the online universe has shaped many if not most aspects of our lives. Gone are the days when a connection to cyberspace was seen as an optional luxury, to the extent that there is now a movement afoot to enshrine such access as a human right.[66] As Paul Bernal has pointed out: "For most people in what might loosely be described as the developed world the internet can no longer be considered an optional extra, but an intrinsic part of life in a modern, developed society."[67]

As with every advance, however, there are drawbacks to our increasing global access to the internet and growing dependence on this technology for an expanding set of diurnal tasks. From love, sex and friendship to banking, grocery shopping and nearly everything in between, the data trail of our private lives can now be tracked online, a reality that has greatly enhanced the threat of surveillance creep. This paradox of a simultaneous facilitating and closing down of freedom is a fact of modern life, and looms large in academic

64 *Barrick Gold Corp v Lopehandia*, (2004) 71 OR (3d) 416, 239 DLR (4th) 577 (quotation immediately preceding start of judgement, citing Matthew Collins, *The Law of Defamation and the Internet* (Oxford: Oxford University Press, 2001) at para 24.02).

65 *Crookes v Newton*, 2011 SCC 47 at para 34, [2011] 3 SCR 269.

66 For more on this development see Michael Karanicolas, "Understanding the Internet as a Human Right" (2012) 10 CJLT 263.

67 Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge: Cambridge University Press, 2014) at 2.

and other discussions of Bill C-51 and similar state initiatives. Davies is downbeat, lamenting 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."[68] Equally pessimistic, Monroe E. Price reports that among civil liberties groups there exists "deep anxiety about the future of freedom of expression itself — a haunting and often undeclared pessimism triggered by the feeling that these same potentially liberating technologies … have instead ushered in an era of surveillance."[69] Richards agrees, cautioning that although the "embrace of digital platforms has been an undeniable force for good, enabling almost anyone with a networked computer or mobile phone to read widely and speak to the world instantaneously … [such platforms] have been designed to create a data trail for each of us of what we think, read, and say privately."[70]

One of the first casualties of this grave new world, then, is privacy, as government actors follow the data trail in pursuit of criminals and other national security threats, at times with the intentional or unwitting assistance of corporations.[71] Although it goes without saying that states should take all reasonable steps to protect their citizens, such strategies do at times appear to overreach. Relying on the well-worn shibboleth of national security, officials in Canada and elsewhere have created instruments like SCISA to the detriment of our fundamental liberties. Arthur J. Cockfield avers: "Canada and other governments are responding to … concerns about security by promoting the use of new technologies by police and/or intelligence officials to locate, track and arrest suspected criminals and/or terrorists."[72] Likewise, in his re-telling of the Snowden saga Greenwald isolates this central feature of post-9/11 thinking. As he argues, the "opportunity those in power have to characterize political opponents as 'national security threats' or even 'terrorists' has repeatedly prov-

68 Davies, *supra* note 30 at 265.

69 Monroe E Price, *Free Expression, Globalism and the New Strategic Communication* (Cambridge: Cambridge University Press, 2015) at 5.

70 Richards, *supra* note 20 at 2.

71 Critics have catalogued the ways in which corporations are complicit in undermining online privacy and free speech. See Austin, *supra* note 6 at 132; Deibert, *supra* note 17 at 197-98; Richards, *supra* note 20 at 174; Jacobs, *supra* note 20 at 2-3; Bernal, *supra* note 67 at 55; Price *supra* note 69 at 34; Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Hamish Hamilton: London, 2014) at 170.

72 Arthur J Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies" (2007) 40 UBC L Rev 41 at 52. John Stuart Mill, in his 1859 tract *On Liberty*, Alan S Kahan, ed (Boston, Bedford / Martin's, 2008) at 30, reminds us that this linking of security and surveillance dates back to the "ancient commonwealths". Lyon also makes this point: "Surveillance is not new. Since time immemorial, people have 'watched over' others to check what they are up to, to monitor their progress, to organize them or to care for them": *supra* note 8 at 22.

en irresistible."[73] This view is shared by Davies, in whose opinion the "new terrorism legislation passed in almost every Western country since 9/11 has been based on the motto of 'everything has changed.'"[74] On the basis of such "[v]ague and unspecified notions of 'national security,'"[75] privacy and freedom of expression are now under attack, in Canada and around the planet.

Within this shadowy world, where one can never be quite certain if one is being watched (especially if one is on the government's radar for whatever reason), the right to freedom of expression can take a significant hit. As various critics have observed,[76] Jeremy Bentham's concept of the Panopticon,[77] a prototype of the Big Brother trope created by Orwell over one hundred and fifty years later,[78] is an apt metaphor for the chilling effects of such surveillance. A prison in which inmates are housed along the perimeter walls and never know if they are being watched by the centrally situated guard, this design was meant to instill a sense of the "apparent omnipresence of the inspector."[79] In a similar way, certain components of Bill C-51 and like legislative instruments could be said to chill expression. Critically, the point here is not that one must be aware that he or she is being monitored but, rather, that the mere reasonable apprehension of being monitored can deter speech. This dynamic, that "even the *perception* … of being surveilled can have a chilling effect,"[80] is a common leitmotif in analyses of the impact of state snooping on online freedom.[81] Like Bentham's prisoners, persons with some realistic sense that they are under scrutiny, and who as a result refrain from making (typing) this or that statement

73 Greenwald, *supra* note 71 at 186.

74 Davies, *supra* note 30 at 263.

75 *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, 23rd Sess, UN Doc A/HRC/23/40 (17 April 2013) at para 58, online: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement>.

76 See Richards, *supra* note 20 at 104; Greenwald, *supra* note 71 at 175.

77 Jeremy Bentham, "Panopticon, or The Inspection House" in John Bowring, ed, *The Works of Jeremy Bentham*, vol 4 (New York: Russell & Russell, 1962) 37.

78 Orwell, *supra* note 11 at 5.

79 Bentham, *supra* note 77 at 45.

80 Jillian York, "The Harms of Surveillance to Privacy, Expression and Association" in *Global Information Society Watch 2014: Communications Surveillance in the Digital Age* 29 at 29, online: <giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf> [*Global Information Society Watch*].

81 For analyses of this chilling effect across different jurisdictions see Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12 Can Crim L Rev 115 at 145; Sunny Skye Hughes, "US Domestic Surveillance after 9/11: An Analysis of the Chilling Effect on First Amendment Rights in Cases Filed against the Terrorist Surveillance Program" (2012) 27:3 CJLS 399 at 400; Demetrius Klitou, *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century* (The Hague: Asser Press, 2014) at 253.

for fear of reprisal, might well be able to argue cogently that their liberties have been abridged.[82]

In the wake of the Snowden leaks much attention has focused on the U.S. government spying undertaken by the National Security Agency, though it has become apparent that Canada too is active in this regard. As has been documented in academic and media circles, CSE (along with the other members of the secretive Five Eyes Alliance[83]) has been busy sorting through huge amounts of intercepted online communications in an effort to thwart potential security threats.[84] Referencing a Canadian "spying initiative" with the code name Levitation, Greenwald and Ryan Gallagher reported that the "Canadian government has launched its own globe-spanning Internet mass surveillance system."[85] According to a Canadian Broadcasting Corporation story two weeks later, "Canada's electronic spy agency sifts through millions of videos and documents downloaded online every day by people around the world, as part of a sweeping bid to find extremist plots and suspects."[86] And while CSE might insist that in "collecting and analyzing metadata [it] does not direct its activities at Canadians or anyone in Canada,"[87] the discovery care of Snowden that CSE tapped into an internet server at a "major Canadian airport" has led experts to challenge this claim.[88] Given these reported covert operations, and

82 For a recent study of "chilling effects theory" see Jonathon W Penney, "Internet Surveillance, Regulation and Chilling Effects Online: A Comparative Case Study" (2017) 6:2 Internet Policy Rev, online: <https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case>. Beyond reviewing the current academic literature on this point, Penney seeks to measure the behavioural impact of web surveillance through a "first-of-its-kind online survey" (at 1).

83 The other four members of this group are the U.S. National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Signals Directorate and New Zealand's Government Communications Security Bureau.

84 In *False Security: The Radicalization of Canadian Anti-Terrorism* (Irwin Law: Toronto, 2015) at 166, Craig Forcese and Kent Roach remark: "We now have the technology to store and mine unprecedented amounts of data. The haystacks are exponentially expanding, but it is also becoming more difficult to find the needles of actionable intelligence that could present a future Air India bombing." See also Lisa M Austin, "Anti-Terrorism's Privacy Slight-of-Hand: Bill C-51 and the Erosion of Privacy" in *After the Paris Attacks*, *supra* note 17, 183 at 186.

85 Ryan Gallagher and Glenn Greenwald, "Canada Casts Global Surveillance Dragnet over File Downloads", *The Intercept* (18 January 2015), online: <https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance>.

86 Amber Hildebrandt, Dave Seglins & Michael Pereira, "CSE Tracks Millions of Downloads Daily: Snowden Documents", *CBC News* (27 January 2015), online: <www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120>.

87 Jim Bronskill, "Canada's Electronic Spy Agency Defends Role in Hunt for Terrorists", *Global News* (28 January 2015), online: <globalnews.ca/news/1799807/canadas-electronic-spy-agency-defends-role-in-hunt-for-terrorists/>.

88 Greg Weston, Glenn Greenwald & Ryan Gallagher, "CSEC used Airport Wi-Fi to Track Canadian Travellers: Edward Snowden Documents", *CBC News* (30 January 2014), online:

federal powers like those authorized under the *Canadian Security Intelligence Service Act*[89] and SCISA's information-sharing regime, it is not unreasonable to suggest that our internet freedoms may potentially be in jeopardy, at home as well as abroad.

This is where section 2(b) could come into play. In cases involving government surveillance of online communication, the chilling of expression flowing from this interference falls precisely within the ambit of a privacy-responsive free speech right. Although the injured party might in this case also attack this privacy violations through section 8, section 2(b) is the preferable option for targeting any resulting chilling effect. To the extent that victims can show that state surveillance impinges on their ability to "express their opinions or communicate with other persons for fear that they will face sanctions,"[90] they could make use of section 2(b), either on its own or in conjunction with section 8. Because "mass surveillance violates both the right to privacy and to freedom of expression,"[91] it makes sense that section 2(b) would feature in any challenge to such activity touching on expression, alongside or instead of search and seizure. In a sense, utilizing section 2(b) thus recalls the failed bid during parliamentary debates over the drafting of the *Charter* to introduce a section 2(e), which if adopted would have guaranteed "freedom from unreasonable interference with privacy, family, home, correspondence, and enjoyment of property."[92] It is noteworthy that the proponents of this doomed section 2(e) project chose "Clause 2," which already housed freedom of expression, for their proposed privacy right, as if confirming in the structure of the *Charter* itself the continuity of these two interests.

5. Freedom of thought

It is easy to forget, in exploring the privacy aspects of section 2(b), that this constitutional provision entails two distinct ideas: freedom of expression and

<www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>. See also Kent Roach, "CSEC's Airport Program: Questions of Legality, Propriety and the Adequacy of Review" (2014) 60:4 Crim LQ 469.

89 *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*].

90 *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin*, 13th Sess, UN Doc A/HRC/13/37 (28 December 2009) at para 34, online: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/178/04/PDF/G0917804.pdf?OpenElement>.

91 Privacy International and Amnesty International, *Two Years After Snowden: Protecting Human Rights in an Age of Mass Surveillance* (4 June 2015) at 3, online: <https://www.privacyinternational.org/sites/default/files/Two%20Years%20After%20Snowden_Final%20Report_EN.pdf>.

92 *Supra* note 27, No 41 at 97.

freedom of thought. While certainly related, these twin concepts are substantively different, a fact that has been overlooked in the Canadian context for a number of reasons. First, both are included within the same section of the *Charter*, which lists "freedom of thought, belief, opinion and expression" in a single phrase as if grouping them together without distinction. However, the coupling of these rights is far from the accepted standard in international human rights instruments. In such instruments, thought and speech are often treated separately, with "freedom of thought, conscience and religion" being distinguished from "freedom of expression".[93] Here, the right to think for oneself, an internal intellectual process, is grouped with other forms of pre-expressive activity, necessary yet antecedent to public, externalized speech. Those who prefer the international model can at least take comfort that the *Charter* incorporates freedom of thought at all. Its predecessor, the 1960 *Canadian Bill of Rights*,[94] refers only to "freedom of speech" (section 1(d)) with no mention of thought whatsoever.

The second reason that freedom of thought (as opposed to expression) gets short shrift in Canadian jurisprudence is the obvious point that, at least until recently, it was far more difficult in practice to control internal ideas than external speech. Although Orwell might speak of "Thought Police"[95] and the possibility of mapping our unspoken impulses and desires, such reach, by government agents or anyone else, might strike one as the stuff of dystopian fiction. This point of view is echoed in Peter W. Hogg's overview of section 2(b), where he explains that the "references to 'thought, belief, opinion' will have little impact, since even a totalitarian state cannot suppress unexpressed ideas," adding that "[i]t is the reference to 'expression' in s. 2(b) that is the critical one, and the word expression is very broad."[96] While it is no doubt correct that the expression piece in section 2(b) gets more attention in constitutional litigation, the right to think freely has taken on greater significance in this "golden age of surveillance."[97] What Richards calls "intellectual privacy,"[98] this ability to think without limits has come under attack in recent years, a development that has of late given this element of section 2(b) more relevance and "impact."

93 See, for instance, the *Universal Declaration of Human Rights*, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71, arts 18-19; *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171 arts 18-19.

94 *Canadian Bill of Rights*, SC 1960, c 44, s 1(d).

95 Orwell, *supra* note 11 at 6.

96 Hogg, *supra* note 61 at Part 43.3. J B Bury, in *A History of Freedom of Thought* (Oxford: Oxford University Press, 1952) at 1, is likewise of the view that one "can never be hindered from thinking what he chooses so long as he conceals what he thinks."

97 Gus Hosein, "Introduction" in *Global Information Society Watch*, *supra* note 80, 9 at 10.

98 Richards, *supra* note 20 at 5.

Long overshadowed by free speech since first debuting on the Canadian constitutional stage in 1982, the freedom of thought guarantee might now be gearing up for its own close-up.[99]

While the section 2(b) jurisprudence is almost exclusively focused on freedom of expression, Canadian courts have on occasion considered freedom of thought as well and, in doing so, have emphasized the privacy component of this right. In *Taylor*, for instance, Dickson C.J.C. accepted that "the freedoms of conscience, thought and belief are particularly engaged in a private setting,"[100] a comment cited by McLachlin C.J.C. in *Sharpe*.[101] More generally, some judgments have underlined the importance of this inward-looking right to individual liberty and the process of self-fulfillment and realization. As articulated by the Supreme Court of Canada, the "right to think and reflect freely on one's circumstances and condition"[102] is central to section 2(b) and forms an "extension of individual liberty."[103] Another forceful endorsement of this facet of section 2(b), and the need to shelter ideas from public scrutiny, is found in *R v Watts*, where the Provincial Court of British Columbia celebrated the realm of private thought. Justice Angelomatis asked: "What could be more implicit in freedom of thought, belief, opinion and expression than the right to hold those beliefs and communicate those opinions privately?"[104] For him, it was "only through the exercise of our privacy rights that we are able to distinguish ourselves from animals. It is only on that philosophical plane that we are truly distinct from other societies and cultures that are either dictatorships or socially constrained cultures."[105]

So why has freedom of thought, formerly largely ignored in the case law, suddenly become relevant in the surveillance context? The answer is that tech-

99 This tendency to valorize speech over thought is evinced by Dickson CJC in *R v Andrews*, [1990] 3 SCR 870 at 879, 77 DLR (4th) 128, when he comments (quoting Cory J.A., then on the Court of Appeal for Ontario): "Freedom of thought is of limited value without the freedom to express that thought."

100 *Taylor*, *supra* note 49 at 937.

101 *Sharpe* (SCC), *supra* note 50 at para 26. In *R v Wong*, 56 CR (3d) 352, 1987 CarswellOnt 88 (WL Can) at para 39 the Court of Appeal for Ontario similarly concludes (in the context of s. 8): "No doubt the greatest expectation of privacy will exist in the home, where there must be freedom to express one's innermost thoughts and feelings."

102 *RWDSU, Local 558 v Pepsi-Cola Canada Beverages (West) Ltd*, 2002 SCC 8 at para 32, [2002] 1 SCR 156.

103 *Lavigne v Ontario Public Service Employees Union*, [1991] 2 SCR 211 at 273, 81 DLR (4th) 545 (quoting the Ontario Court of Appeal).

104 *R v Watts*, 2000 BCPC 191, [2000] BCJ No 2721 (QL) at para 9.

105 *Ibid* at para 10. This insistence on the primacy of private thought is also reflected in the child pornography exemptions carved out by the Supreme Court of Canada in the *Sharpe* decision, *supra* note 50 at para 108.

nological advances have rendered the once seemingly impossible task of reading minds more reality than fantasy, as online data trails expose private thoughts and desires to state (and corporate) scrutiny. Richards identifies such scrutiny as a fact of contemporary life: "although it is an old idea, intellectual privacy has remained under-appreciated and underdeveloped … not because intellectual privacy is trivial, but because until very recently, it has been difficult as a practical matter to interfere with the generation of ideas."[106] As he discerns, while "in the past, access to ideas has come principally from print media," today this access is web-based so that "gradually, over the decades, technologies have come to mediate our thinking, reading, and communications."[107] Cockfield too is alert to this new normal, warning that while "governments and businesses have always watched us to a certain extent … new surveillance technologies exponentially increase the ability of others to gather, store and index information about us."[108] Ultimately, this heightened scrutiny results in self-censorship: "Greater scrutiny could make us take greater care before we visit a website or tap out a few thoughts on our word processors. If an individual thinks that her activities … will somehow be stored and potentially used against her in the future, she may change her behaviour."[109]

According to Richards, "if we are interested in freedom of speech and the ability to express new and possibly heretical ideas, we should care about the social processes by which these ideas are originated, nurtured, and developed."[110] This statement is particularly apropos in light of present-day concerns over government surveillance, and rings true in any jurisdiction in which internet privacy is under siege. While it might once have been true that speech, not thought, could be caught by the state's monitoring apparatus, technological developments, in combination with post-9/11 security malaise, have created a "perfect storm" in which one's private musings may no longer be safe. David Kaye, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, brings this issue to the at-

106 Richards, *supra* note 20 at 96.

107 *Ibid* at 97, 175.

108 Arthur J Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance" (2003) 29:1 Queen's LJ 364 at 395. Jeffrey Rosen agrees in *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, 2000) at 7: "For as thinking and writing increasingly take place in cyberspace, the part of our life that can be monitored and searched has vastly expanded…On the Internet, every Web site we visit, every store we browse in, every magazine we skim, and the amount of time we spend skimming it, create electronic footprints that increasingly can be traced back to us, revealing detailed patterns about our tastes, preferences, and intimate thoughts."

109 Cockfield, *ibid* at 395.

110 Richards, *supra* note 20 at 103.

tention of the U.N. Human Rights Council in a 2015 report. Insisting on the necessity of protecting both speech and thought, he draws attention to the fact that the "right to hold opinions without interference also includes the right to form opinions."[111] "[T]argeted and mass" systems of surveillance, he continues, "may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes."[112]

In addition to speech issues resulting from online surveillance, then, the privacy aspect of section 2(b) could likewise assist with respect to any freedom of thought violation. A litigant relying on section 2(b) could focus on external and internal processes, addressing both the impact of government monitoring on both expression as well as embryonic thoughts in the process of development. Given the ascendance of our surveillance society, section 2(b) could serve double duty in this regard, as those deterred from speaking and/or internet surfing could add this *Charter* provision (along with section 8 and, possibly, section 7) to their constitutional tool kit. Sometimes, despite the popular saying, more is more, not less, and it is difficult to understand how expanding the range of legal responses in Canada to such government-induced deterrence is a bad thing, provided that it has some basis in law and, ideally, a chance of success. And it would appear, as I discuss below, that the CCLA, CJFE and BCCLA have all evinced faith in this approach by featuring it in legal challenges to Canada's 2001 and 2015 anti-terrorist legislation. Turning to review these judicial proceedings, which continue to make their way through Canadian courts, I will provide an overview of how section 2(b) is currently being deployed in connection with privacy rights.

6. Litigation featuring a privacy-centric approach to section 2(b)

As with any constitutional argument, the rubber really hits the road when such ideas are battle tested in litigation, an indication that (at least in theory) the parties have sufficient confidence in particular strategies to submit them to judicial scrutiny. One of the interesting things about cases like *Spencer*, *Sharpe* and *Taylor*, which recognize the intersection of speech and privacy, is that none

111 *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, 29th Sess, UN Doc A/HRC/29/32 (22 May 2015), at para 21, online: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/pdf/G1509585.pdf?OpenElement>.

112 *Ibid*.

of them feature or otherwise address the privacy-inflected approach to section 2(b) outlined above. *Spencer*, the most recent and arguably on point of these Supreme Court of Canada decisions, is actually a section 8 proceeding and, despite its forward-looking and novel treatment of anonymity and freedom of expression, never formally considers section 2(b) itself. Only one completed *Charter* challenge has made use of section 2(b) thus: C*CLA v Canada*,[113] which sought to attack surveillance powers in the *CSIS Act*.[114] Abella J.A. (as she then was), while concurring with the majority of the Ontario Court of Appeal that the case should be dismissed on standing and evidentiary grounds, allowed that the case "raises serious questions" about the impact of such powers on section 2(b) rights.[115] It is reasonable to assume that, should Canadians continue to encounter privacy-invasive legislation of the sort challenged in *CCLA v Canada*, new legal proceedings will be initiated to stem the tide of invasive government action.

While there exists little in the way of concluded litigation on point, two *Charter* challenges (one comprised of two distinct proceedings) have been commenced which illustrate how section 2(b) can be utilized with a privacy focus to combat online surveillance. A challenge to Bill C-51, initiated jointly in July 2015 by the CCLA and CJFE,[116] covers a great deal of legal ground in attacking five separate aspects of the omnibus statute. In addition to impugning SCISA and speech limiting amendments to the *Criminal Code*, the applicants zero in on the *Secure Air Travel Act* and revisions to the *Immigration and Refugee Protection Act* and the *Canadian Security Intelligence Act*.[117] This lawsuit,

113 *Corporation of the Canadian Civil Liberties Association v Canada (AG)*, 74 OR (2d) 609, 1990 CanLII 6715 (H Ct J) [*CCLA v Canada* (H Ct J)]; *Corporation of the Canadian Civil Liberties Association v Canada (AG)*, 40 OR (3d) 489, 1998 CanLII 6272 (CA) [*CCLA v Canada* (CA)].

114 *CSIS Act*, *supra* note 89.

115 As Abella J.A. said of the merits: "The information contained in C.C.L.A.'s supporting affidavits raises serious questions about whether the constitutionally protected rights of citizens to engage in lawful expression… may be compromised or threatened under the authority of the *Canadian Security Intelligence Act*.": *CCLA v Canada* (CA), *supra* note 113 at 522. She suggested that government surveillance can cause violations of s. 2(b) and that the CCLA did adduce some (though, apparently, not enough) evidence to this effect. "There is no question," Abella J.A. wrote, "that the perception of C.S.I.S. intervention was, to say the least, unsettling to the people involved and potentially inhibiting": *ibid*. At an earlier point of the proceeding Justice Potts of the Ontario High Court of Justice characterized the claim in these terms: "individuals proposing to do no more than engage in advocacy and dissent do not always know whether their lawful activities will be monitored" and the "cautious among them may, and do, choose to refrain from engaging in legitimate political activities for fear of becoming objects of CSIS surveillance.": *CCLA v Canada* (H Ct J), *supra* note 113 at 619.

116 *CCLA v Canada (AG)* (21 July 2015), Toronto, CV-15-532810 (Ont Sup Ct) (Notice of Application), online: <https://ccla.org/cclanewsite/wp-content/uploads/2015/08/Issued-Notice-of-Application-Bill-C-51-C1383715xA0E3A.pdf> [CCLA Notice of Application].

117 *Ibid* at paras 3-4.

as explained by the moving parties, was commenced because of the "disturbing implications for free speech, privacy" and the "powers of government"[118] presented by Bill C-51. According to Tom Henheffer, CJFE Executive Director, Bill C-51 "unjustifiably infringes on the rights of all Canadians without making our country any more secure, and must be struck down."[119] For her part, Sukanya Pillay, Executive Director of the CCLA, makes clear that this law is being opposed because it "creates broad and dangerous new powers, without commensurate accountability."[120]

While this proceeding has yet to advance to a hearing, certain aspects of its approach to section 2(b) are evident from the Notice of Application, particularly as it relates to SCISA and the *Criminal Code* amendments. These parts of the pleadings disclose both a conventional approach to section 2(b), along with a parallel use of this provision anchored in privacy considerations. The former centres on section 83.221 of the *Criminal Code*, which outlaws advocating for or promoting the "commission of terrorism offences in general." Here the applicants allege a narrowing of expression, characterizing section 83.221 as criminalizing "constitutionally protected speech and other expressive activities."[121] This traditional leveraging of section 2(b) is supplemented, in relation to SCISA, with an argument based entirely in a privacy framework. Taking issue with the breadth of the SCISA information-sharing powers, the CCLA and CJFE claim that the "invasive state archiving and information sharing" between government departments will "chill" and "deter legitimate expression."[122] Such "secret" intelligence activity is portrayed in a manner evoking Bentham's Panopticon, as those under observation cannot "determine (or challenge in any meaningful way) how their activities and conduct have been … construed … [or] shared and used"[123] by Ottawa.

On April 1, 2014, more than a year prior to Bill C-51 coming into force and the start of the CCLA/CJFE litigation, the BCCLA commenced a class action challenging sections 273.65, 273.68 and 273.7 of the *National Defence*

118 Canadian Civil Liberties Association, Media Release, "CCLA & CJFE Mounting Charter Challenge Against Bill C-51" (21 July 2015), online: <https://ccla.org/ccla-and-cjfe-mounting-charter-challenge-against-bill-c-51>.

119 *Ibid*.

120 *Ibid*.

121 CCLA Notice of Application, *supra* note 116 at paras 24, 26. The CCLA and CJFE argue that this concept is "overly vague, broad and imprecise" and that, consequently, it exerts a "chilling effect on freedom of expression and association, even if no prosecution is ever brought": *ibid* at paras 26-27.

122 *Ibid* at para 34.

123 *Ibid* at paras 34-35.

Act,[124] legislative provisions relating to CSE surveillance efforts.[125] Later that year, the BCCLA initiated a second proceeding, similar in scope to its first case but packaged as a regular action and dropping any reference to section 273.7.[126] Central to both claims, advanced on the basis of sections 2(b) and 8 of the *Charter*, are the CSE powers granted by section 273.65 to "intercept private communications."[127] As stipulated in the statute, such powers are available for two purposes: "obtaining foreign intelligence" or "protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference."[128] Regarding the former, section 273.65(2) requires that any CSE interception must be "directed at foreign entities located outside Canada" and can only be "used or retained if they are essential to international affairs, defence or security."[129] Ministerial authorizations are needed to engage in this monitoring activity, though section 273.68 is vague on timelines or the possibility of multiple renewals, other than specifying that "[n]o authorization or renewal may be for a period longer than one year."[130] According to the BCCLA's October 27, 2014 Statement of Claim, the "Minister issued at least 78 Authorizations between 2002 and 2012."[131]

The constitutional arguments raised by the BCCLA in the April and October 2014 proceedings are nearly identical and foreground the privacy implications stemming from this interception of online communications. In impugning sections 273.65 and 273.68, introduced into the *National Defence Act* via the 2001 *Anti-Terrorism Act*,[132] the petitioners make interference with the private sphere a central issue, which they tackle not merely through section 8 but equally by means of section 2(b). As alleged by the BCCLA in its October 2014 Statement of Claim, the "impugned provisions and Authorizations that purport to provide [CSE] with legal authority to intercept the private communications of persons in Canada are an infringement of s. 2(b)."[133] Complementing the BCCLA's use of section 8, on the basis of which such surveillance is attacked

124 *National Defence Act*, RSC 1985, c N-5, ss 273.65, 273.68 and 273.7.

125 *BCCLA v Canada (AG)* (1 April 2014), Vancouver, T-796-14 (FCTD) (Statement of Claim), online: <https://bccla.org/wp-content/uploads/2014/04/20140401-Statement-of-Claim-Class-Action-Proceeding.pdf> [BCCLA April Statement of Claim].

126 *BCCLA v Canada (AG)* (27 October 2014) Vancouver, T-2210-14 (FCTD) (Statement of Claim), online: <https://bccla.org/wp-content/uploads/2014/12/20141027-CSEC-Statement-of-Claim.pdf> [BCCLA October Statement of Claim].

127 *National Defence Act*, *supra* note 124 at s 273.65(1), (3).

128 *Ibid* at s 273.65(3).

129 *Ibid* at s 273.65(2).

130 *Ibid* at s 273.68(1).

131 BCCLA October Statement of Claim, *supra* note 126 at para 26.

132 *Anti-Terrorism Act*, SC 2001, c 41.

133 BCCLA October Statement of Claim, *supra* note 126 at para 38.

as violating "reasonable expectation[s]" regarding the use and dissemination of personal information, the right to free speech is vital to this litigation. Beyond targeting the interception of speech, section 2(b) is also enlisted to challenge CSE's powers to "collect, analyze, retain, use and/or distribute internationally metadata that is associated with or produced by persons in Canada."[134] In harnessing section 2(b) in terms of information sharing and expression, these BCCLA lawsuits reflect the breadth of privacy-related possibilities attaching to this *Charter* right.

The CCLA/CJFE and BCCLA proceedings are ongoing and it is difficult to predict if they will make it to the hearing stage, let alone how their privacy-centric uses of section 2(b) will be received by the courts. Whatever its outcome, such advocacy represents a recent development in *Charter* litigation in which section 2(b) is pleaded in response to the chilling effects of surveillance and related information-sharing activities. Moreover, while the statutory provisions at issue in these cases do not exclusively concern online themes, these challenges have the potential to shine a light on the internet dimension of state surveillance of concern to Canadians. Though the CCLA/CJFE Notice of Application does not refer explicitly to the Web (other than citing the *Criminal Code* "internet deletion provisions"[135]), its invoking of the "era of 'big data' information processing"[136] in connection with SCISA is a nod to the massive data trails subject to monitoring. The BCCLA statements of claim are more directly on point, and speak of "metadata" as "expressive content that is protected under section 2(b)."[137] Together, these lawsuits signal an expanded potential for the free speech guarantee, a modern take on this right responsive to our privacy perils in cyberspace.

7. Conclusion

In this paper I have traced the connections between privacy and expression and have outlined how this link, acknowledged by Canadian courts, has been incorporated into section 2(b) litigation targeting invasive government surveillance. This highlighting of the privacy-speech nexus is timely, given our increasing dependence on the internet and the ease with which both thoughts and speech can now be intercepted online. Responding to this twenty-first century threat, which has gripped the popular imagination, advocates have

134 *Ibid* at para 39.

135 CCLA Notice of Application, *supra* note 116 at para 9.

136 *Ibid* at para 35.

137 BCCLA April Statement of Claim, s*upra* note 125 at para 45; BCCLA October Statement of Claim *supra* note 126 at para 37.

taken hold of this vision of section 2(b) in their defence of the private sphere. As Abella J.A. asserted in *CCLA v Canada*: "It goes to the heart of an open democracy that members of the public are, and perceive that they are, free from unwarranted government surveillance when they are engaging in lawful, even if provocative, activity."[138] While this 1990s case may not have been a win for the CCLA, its forceful attack on CSIS's "exceptional legislative tool"[139] set the stage for future challenges, including the ongoing BCCLA and CCLA/CJFE lawsuits surveyed above. And, as concerns regarding online state surveillance continue to grow in our post-9/11 reality (the Court of Appeal rendered its *CCLA v Canada* decision in 1998), it seems likely that judges will remain ever more mindful of digital privacy.

Time will tell if Bill C-51 represents a low water mark in recent Canadian law-making efforts or whether it constitutes merely the first gambit in the ongoing development of federal surveillance powers. The Trudeau Liberals, since capturing a majority government in October 2015, have yet to take steps toward repealing any part of the *Anti-Terrorism Act, 2015*, despite promises to do so. As announced on the official party website: "We will repeal the problematic elements of Bill C-51, and introduce new legislation that better balances our collective security with our rights and freedoms."[140] Among the eight priorities pledged in this context is the assurance that such legislation will "guarantee that all [CSE] warrants respect the *Charter*," reign in CSE "powers by requiring a warrant to engage in the surveillance of Canadians," ensure that "Canadians are not limited from lawful protests and advocacy" and assemble an "all-party national security oversight committee."[141] Though certainly a start, the value of some of these commitments remains an open question. Even Parliament's Standing Committee on Public Safety and National Security would seem to be running out of patience. In its May 2, 2017 report *Protecting Canadians and their Rights: A New Roadmap for Canada's National Security*, which offers up more than 40 recommendations for updating SCISA and related statutes, the Committee rejects the "false dichotomy" between "national security efforts"

138 *CCLA v Canada* (CA), *supra* note 113 at 522.

139 *Ibid*.

140 Official Liberal Party website, online: <https://www.liberal.ca/realchange/bill-c-51/>. This need for balancing national security interests against *Charter* rights is also trumpeted in the *Green Paper*, *supra* note 13 at 6: "In protecting national security, the Government must find an appropriate balance between the actions it takes to keep Canadians safe and the impact of those actions on the rights we cherish."

141 *Ibid*. It is at present too soon to judge whether Bill C-59 ("An Act respecting national security matters"), tabled in the House of Commons on June 20, 2017, will (assuming it passes into law) substantively address issues of concern to groups like the CCLA, the BCCLA and CJFE. Online: <http://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/first-reading>.

and "uphold[ing] human rights."[142] In the meantime, one can take comfort in the expanding reach of section 2(b), which remains poised to defend our privacy as well as our speech.

142 Online: <https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/report-9/page-105#29>.