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

by

David Maurice Tortell

A thesis submitted in conformity with the requirements for the degree of Master of Laws

Faculty of Law
University of Toronto

© Copyright by David Maurice Tortell 2017
Surfing the Surveillance Wave: Online Privacy, Freedom of Expression and the Threat of National Security

David Maurice Tortell

Master of Laws

Faculty of Law
University of Toronto

2017

Abstract

This thesis explores the emergence of s. 2(b) of the Charter as a response to privacy breaches flowing from government surveillance of online personal information. My study begins by examining two competing views of the relationship between free speech and privacy: opposites in conflict versus complimentary, interconnected rights. I then proceed to look at privacy itself, addressing difficulties faced in defining this concept and ways in which privacy has been read into, and excluded from, the Charter. Next, I focus on aspects of s. 2(b), including freedom of thought, the chilling effects of surveillance and jurisprudence like the 2014 Supreme Court of Canada R. v. Spencer decision which isolates privacy as a vehicle for expression. I conclude by reviewing the advantages and challenges of this privacy-centric approach to s. 2(b), and discuss two ongoing Canadian constitutional lawsuits which adopt this approach in attacking Bill C-51 and other national security legislation.
Acknowledgments

I am very grateful to my thesis supervisor Professor Kent Roach for his guidance, support and kind assistance at every stage of this project. Working with and learning from him has truly been a pleasure, and I have benefited enormously from his total command of the law and his generosity of spirit. I would also like to thank the entire LL.M. program team, and in particular Associate Dean Mariana Mota Prado, Assistant Dean Judith McCormack, Tracey Gameiro and Whittney Ambeault, for making this degree a rich intellectual and personal experience.
Likewise, I am indebted to my SJD advisor Diego Garcia-Ricci for helping me navigate the writing process and making himself available for questions and coffee. And, lastly, a thousand thanks to Elana, my wife and best friend, for putting up with me throughout this adventure and providing encouragement and humour along the way.
# Table of Contents

Abstract ......................................................................................................................................................... ii
Acknowledgments ........................................................................................................................................ iii
Table of Contents ........................................................................................................................................ iv
INTRODUCTION ........................................................................................................................................... 1

CHAPTER 1 .................................................................................................................................................. 5
1 Introduction .................................................................................................................................................. 5
2 Privacy versus freedom of expression ...................................................................................................... 10
  2.1 Constitutional law and the question of balance ................................................................................. 10
  2.2 Private lives and public speech ........................................................................................................... 17
  2.3 The right to be forgotten ..................................................................................................................... 23
3 Privacy as a mechanism for freedom of expression .................................................................................. 29
  3.1 From clash to continuity of rights ........................................................................................................ 29
  3.2 Anonymity, expression and the internet .............................................................................................. 35
4 Spencer and the privacy-speech continuum .............................................................................................. 41
  4.1 Introduction to Spencer decision ......................................................................................................... 41
  4.2 Spencer advances case law concerning privacy and speech .............................................................. 47
5 Conclusion .................................................................................................................................................... 53

CHAPTER 2 .................................................................................................................................................. 57
1 Introduction .................................................................................................................................................. 57
2 Privacy ......................................................................................................................................................... 62
  2.1 The parameters of privacy .................................................................................................................... 62
  2.2 Privacy rights abroad and (almost) in Canada ..................................................................................... 67
  2.3 Reading privacy into the Charter ........................................................................................................ 73
3 Freedom of expression ............................................................................................................................... 79
  3.1 The free speech-privacy connection ..................................................................................................... 79
  3.2 Grave new world of online surveillance .............................................................................................. 85
  3.3 Freedom of thought .............................................................................................................................. 92
4 From concept to courtroom ........................................................................................................................ 98
  4.1 Two cases featuring a privacy-centric vision of s. 2(b) ...................................................................... 98
  4.2 Advantages and potential challenges in the courtroom ................................................................. 103
5 Conclusion .................................................................................................................................................. 110

CONCLUSION .............................................................................................................................................. 113

BIBLIOGRAPHY .......................................................................................................................................... 116
INTRODUCTION

In this thesis I explore the connections between privacy and freedom of expression, and argue that s. 2(b) can effectively be used, under certain circumstances, as a constitutional tool in response to online government surveillance. While speech and privacy have traditionally been characterized in oppositional terms (a classic view encapsulated in defamation law, where freedom of the press is balanced against the right to privacy), I explore how privacy can at times facilitate and constitute a pre-condition for speech. Canvassing a broad range of examples, within and beyond the confines of black letter law, I explore the ways in which these two rights have come into conflict with and complemented each other over the course of several centuries. Similarly, I discuss how Canadian courts have wrestled with these twin interests and have, despite a prevailing tendency to view them as opposites, on occasion underlined their complementarity. Regarding this last point, I focus in particular on the 2014 Supreme Court of Canada decision in R. v. Spencer,\(^1\) in which Cromwell J. affirms the fundamental importance of anonymity as a vehicle for expression. On the basis of this judgment, and other rulings rendered by this and other Canadian courts, I examine how s. 2(b) can be read through a privacy lens, an approach which, as I detail, is already being deployed in Charter challenges to national security legislation commenced by the Canadian Civil Liberties Association (“CCLA”) and the British Columbia Civil Liberties Association (“BCCLA”).

Underlying this privacy-centric approach to s. 2(b) is a concern with federal government legislative initiatives which have caused much concern amongst journalists, lawyers, civil society groups and, more generally, broad cross-sections of Canadian society. Much of this

\(^1\) R v Spencer, 2014 SCC 43, [2014] 2 SCR 212 [Spencer].
recent attention has focused on Bill C-51, and the ways in which is has in the minds of many, in amending and creating laws, undermined basic Canadian liberties. Just as troubling, though, are predecessors to this omnibus statute, like the Anti-Terrorism Act, 2001 (“ATA 2001”), which itself ushered into existence a suite of surveillance and related powers making it easier for Ottawa to gain access to our private speech and thoughts. Given these invasive monitoring tactics, which would appear to mushroom with each passing Parliamentary season, Canadians (and particularly those who, due to political or related activities, are known to the authorities and are thus more likely to be monitored) should exercise all available options in protecting their internet privacy against such incursions. It is in this spirit that I approach s. 2(b) and propose that, in response to this developing constitutional problem, it makes good sense to marshal the freedom of expression right in our continuing fight against Big Brother. I argue that, combined with other available Charter remedies, principally ss. 7 and 8, s. 2(b) affords an effective instrument, especially with respect to internet surveillance and censorship, in this struggle for online independence.

This thesis is divided into two chapters, each of which are further subdivided into sections touching on a range of connected issues. Chapter one opens with an analysis of two principal ways in which the relationship between privacy and free speech can be understood, both as conflicting rights and, largely in terms of anonymity, as complimentary interests. Addressing the first paradigm, I explore how the Charter, and the various tests which have been created to assist in its interpretation and application, are themselves structurally defined through conflict and

---

2 Anti-Terrorism Act, 2015, SC 2015, c 20.
3 Anti-Terrorism Act, SC 2001, c 41.
tension. I also at this stage consider how Canadian courts have regularly conceived of privacy and speech in such terms and explore the so-called right to be forgotten, which I argue exemplifies this overriding sense of the incommensurability of these rights. I next turn to address the second perspective, anchored in continuity and symbiosis, and trace its development in case law and non-legal sources in a variety of contexts. In the course of discussing this alternative model I review the history and challenges of anonymity and examine aspects of hacktivist culture (and the group Anonymous in particular), which I argue embodies this intersection of privacy and speech. Chapter one closes with a study of *Spencer* and other Canadian judgments which confirm this intersection of rights. Additionally, by way of conclusion, I identify s. 2(b) as a helpful tonic to state intrusions into the online private sphere, and reference current events and litigation relevant to this constitutional strategy.

I pick up this thread in chapter two, where I set out more fully my argument that s. 2(b) constitutes an effective response to state surveillance and offers “value added” beyond the privacy protections afforded by ss. 7 and 8 of the *Charter*. I begin this second half of the thesis by looking at a range of privacy issues, such as difficulties flowing from efforts to define this concept, global perspectives on privacy and ways in which privacy has been read into and excluded from the Canadian constitution. In addressing this last point, I focus in part on pre-*Charter* Parliamentary debates (thus far largely unreported, based on my research) relating to ill-fated efforts to create a stand-alone privacy right within s. 2 of the *Charter*. I then turn my attention to s. 2(b), addressing topics like the expansive interpretation of this provision by Canadian courts, the chilling effects of surveillance and the impact of our slavishness to the internet, and the ensuing data trail, on freedom of thought. The thesis closes with an analysis of
ongoing CCLA and BCCLA challenges to several privacy invasive national security laws, including but not limited to Bill C-51, on s. 2(b) grounds, so as to track in real time this approach to freedom of expression in present day courtrooms. As well, I pause in the final section of chapter two to consider the advantages and potential evidentiary challenges flowing from this privacy specific use of s. 2(b), both from a procedural and substantive point of view.

Through this project I hope to shed light on what I characterize as an emerging and highly relevant yet underappreciated facet of s. 2(b). As I suggest, this vision of free speech is especially apposite at this moment in time, as our lives continue to migrate further online and state surveillance shows no signs of letting up anytime soon. It is generally never a bad thing to have more rather than less protection in any given context, as I argue at various points below, and I pitch this privacy reading of s. 2(b) as merely another arrow in our constitutional quiver. Although one might, depending on the facts, rely only on this Charter provision in tangling with the authorities, I point out that it will sometimes make sense to combine it with another prong of attack (as has been done in the CCLA and BCCLA cases, which plead s. 2(b) in conjunction with s. 8). Either way, this deployment of free speech principles assists in flagging that privacy consists of more than reasonable expectations, a reality which, as I remark in chapter two, is at times obscured by the traditional pairing of privacy and s. 8. Ultimately, then, as well as isolating a neglected aspect of s. 2(b), I seek simultaneously to trace how our understanding of the private sphere is currently expanding in reaction to the threat of government surveillance. Such a shift, I propose, is occurring before our very eyes, as reflected in case law and litigation, and I hope in what follows to provide a glimpse into this contemporary laboratory of constitutional change.
CHAPTER 1
R. V. SPENCER AND THE BRIDGING OF PRIVACY AND EXPRESSION

1 Introduction

One might suggest that this is a golden period for privacy and free speech, two rights which have over the last number of years featured prominently in the courts of law and public opinion across many topics and jurisdictions. Following the explosive 2013 Edward Snowden National Security Agency leaks, which confirmed the existence of government sanctioned surveillance programs in the United States, Europe and elsewhere, much debate was triggered regarding the implications of this intrusion into the realm of personal telephonic and electronic communications which many had previously assumed to be private. Likewise, the brutal murders of eleven people at the start of 2015 generally thought to have been motivated by satirical representations of Islam in Charlie Hebdo, a provocative and often controversial French weekly newspaper, generated a flurry of analysis across and beyond academic circles about the purpose and limits of freedom of expression. In Canada, the introduction of Bill C-51 by the Harper Parliament caused free speech and privacy advocates to throw up their hands in frustration. By introducing legislative amendments and creating new laws like the Security of

---

5 Ibid.
6 Online: <https://charliehebdo.fr>.
7 For a recent example of such analysis see Kent Roach & Craig Forcese, False Security: the Radicalization of Canadian Anti-Terrorism (Toronto: Irwin Law, 2015).
8 Ibid.
Canada Information Sharing Act ("SCISA") said by some to trench on such rights, this omnibus statute brought these civil liberties into sharp focus from coast to coast to coast, within and outside the courtroom, and underscored their current relevance in the Canadian context.

In examining these two rights, whether through a historical lens or in terms of contemporary legal developments, one observes that they intersect at various points and, further, that their relationship to one another can differ significantly depending on the circumstance. While in some cases privacy and free speech are at odds with one another and require balancing, other situations radically alter this relationship such that the second is facilitated, not stymied, by the first. Thus, for example, a journalist seeking to write about a particular person may well be confronted by that person’s wish not to be discussed in the news item, a defining dynamic of many defamation proceedings. As the Supreme Court of Canada has confirmed: “While freedom of expression is a fundamental freedom protected by s. 2(b) of the Charter, courts have long recognized that protection of reputation is also worthy of legal recognition." Beyond this specific tension, however, in other circumstances the ability to speak freely itself hinges on privacy, a long-standing reality of particular import today given that, at least theoretically, anonymous speech is available to anyone with a computer and an internet connection. Indeed, our conquest of cyberspace and the ubiquity of online platforms have foregrounded these two frameworks (oppositional versus facilitative) within which to understand what might be called the free speech-privacy matrix, a development which continues to shift our cultural and legal perspectives and our understanding of liberty and autonomy.

---

9 Security of Canada Information Sharing Act, SC 2015, c 20, s 2 [SCISA].
A review of the relevant case law and commentary makes clear that, generally speaking, freedom of expression and privacy have been portrayed as opposites in constant tension, not unlike protons and electrons. This fact is isolated by Eric Barendt, who characterizes this “traditional perspective concerning the relationship of these two fundamental rights” as a “clash of rights, which must be resolved either in favour of the privacy right or of the right to freedom of speech.”

To be sure, as one scans the Canadian jurisprudence on point this “traditional perspective” is visible at every turn, as speech and privacy are set up as antipodes at opposite ends of the constitutional spectrum. While Canadian courts have been careful, as in the excerpt from *Grant v. Torstar Corp.* above, to herald the importance of each of these interests, much of their analysis involving free speech and privacy is fueled by notions of difference, not similarity. As is canvassed more fully below, these decisions have largely been focused on the principle that “claims for the protection of privacy may give rise to competing claims” and that “[f]oremost [amongst such claims] are claims for the protection of freedom of expression and freedom of the press.”

By and large, the Supreme Court of Canada and other courts, to the extent that they have addressed the interplay of these rights, have ignored, and certainly not enshrined, this alternative reading of this relationship as one marked by continuity and symbiosis.

---


12 *Jones v Tsige*, 2012 ONCA 32 at para 73, 108 OR (3d) 241 [*Jones*].
Until, that is, the Supreme Court of Canada released its *R. v. Spencer* decision in 2014. With this judgment the court upholds the principle that, in certain circumstances, privacy facilitates self-expression and should on this basis be afforded legal protection. Cromwell J., in explaining that anonymity is “particularly important in the context of Internet usage” and can be “claimed by an individual who wants to present ideas publicly but does not want to be identified as their author,”\(^{13}\) expands the law on constitutional free speech protections without ever, it is worth noting, making reference to s. 2(b) of the *Canadian Charter of Rights and Freedoms*.\(^{14}\) Beyond its importance as a s. 8 case, then, *Spencer* is also noteworthy for what it says about the commonalities linking privacy and expression (and the essential related concept of freedom of thought), a finding altogether contrary to the more conventional, oppositional view of these rights. While much of the scholarly writing on *Spencer* has focused on its finding of a reasonable expectation of privacy in one’s internet subscriber information,\(^{15}\) it is equally pivotal in highlighting the continuity of speech and privacy, especially in terms of online activity.

Despite the fact that Cromwell J.’s analysis of such issues constitutes only one of several parts of his ruling, it nonetheless signals a tipping point in the development of Canadian jurisprudence on s. 2(b) and the private sphere.

In this chapter I argue that *Spencer* marks a watershed moment because, in addition to the way in which it alters the parameters of s. 8, it also makes plain in an explicit and novel way the extent to which speech can constitutionally flow from, not merely present a foil to, privacy. Unlike

---

\(^{13}\) *Ibid* at para 45.


\(^{15}\) *Ibid* at para 66.
Grant and other defamation (and other) cases in which these rights are set up as “two conflicting values” in need of “balancing,”

this 2014 Supreme Court of Canada judgment, in a manner distinct from earlier Canadian decisions, tethers privacy to speech. For Cromwell J., privacy is a constitutional safeguard which facilitates and may even render possible speech, a position running counter to the balance of rulings on point. Equally significant, perhaps, is the fact that this great stride in freedom of expression law has nothing to do, strictly speaking, with s. 2(b), since it never formally addresses this Charter provision. This does not mean that Spencer is without application outside of the search and seizure domain, and I conclude by proposing that the intersection of privacy and speech, as set forth by Cromwell J., be imported into s. 2(b) proper. I argue that that such an expansion of s. 2(b) to include a privacy component (like that found in s. 8 and read into s. 7) makes particularly good sense at present, in light of contemporary concerns over state surveillance and its impact on expression.

In what follows I trace the manner in which both versions of the relationship between privacy and freedom of expression have, historically and more recently, manifested themselves in various ways and have in turn been defined by Canadian courts. I first examine what Barendt characterizes as the “traditional perspective”

of these rights “in conflict” and the balancing function central to this vision of speech and privacy. As well as focusing on this “requisite balancing of values,” I will at this juncture also comment on contemporary developments in

---

16 Grant, supra note 10 at paras. 3, 143.
17 Supra note 11 at 11.
19 Hill v Church of Scientology of Toronto, [1995] 2 SCR 1130 at para 121, 126 DLR (4th) 129 [Hill].
what has come to be known as the right to be forgotten and the ways in which Canadian constitutional law is itself animated through concepts of balancing. Next, I consider privacy as an enabler of speech, particularly with respect to anonymity, as illustrated in earlier cultural moments and as presently embodied in the work of groups like Anonymous and other hacker collectives. Finally, I review *Spencer* and related case law in light of these foregoing issues and, on the basis of such jurisprudence, I identify a shift in law anchored in this second approach to speech and privacy. This chapter concludes by proposing that this shift, articulated in *Spencer* in relation to s. 8, be more widely read into s. 2(b), a nascent constitutional strategy (explored in chapter two) adopted in a handful of ongoing *Chartter* challenges focused on privacy and the twin pillars of freedom of speech and thought.

2 Privacy versus freedom of expression
2.1 Constitutional law and the question of balance

Before turning to examine the way in which privacy and free speech are themselves often defined in terms of balancing and conflict, I pause first to reflect on the more general emphasis on balance evinced throughout Canadian constitutional law. This recurring tendency, far from being limited to the delicate balancing of these two specific rights, is evident in many facets of *Chartter* adjudication and mechanics and constitutes a broader framework within which this weighing takes place. Such an exercise, at times described in terms of proportionality or, as Fish

---

20 To be clear, in arguing thus I do not mean to imply that I reject the possibility of a tension existing between speech and privacy or that, in instances of such tension, a judicial balancing of competing rights is unhelpful. On the contrary, *Grant* and other decisions discussed below underscore the reality of such conflict and the necessity of adjudicating these disputes in as fair and inclusive a manner as possible. In valorizing Cromwell J.’s approach to privacy and expression and proposing that his facilitative view be imported into the s. 2(b) context, I intend simply to outline one additional means through which one might respond to allegations of government surveillance and related activity which have of late aroused much discussion and debate.
J. puts it in *R. v. C. (R.)*, as a “constitutional compromise,”\(^{21}\) is at the centre of much of the analysis undertaken by courts and others. It is readily discernable in the very structure of the *Charter*, where at various points one is required to negotiate competing interests, including but not limited to what is perhaps the ultimate question: can an acknowledged rights violation be trumped by a “pressing and substantial” government objective?\(^{22}\) As Grégoire C. N. Webber indicates, “we have come to see constitutional rights only through the prism of proportionality and balancing” and, in his view, contemporary “constitutional rights scholarship and jurisprudence [are] engulfed by the discourse of balancing and proportionality.”\(^{23}\) He adds: “the claim that constitutional law has entered the age of balancing—that it embraces a discourse and practice of balancing—is no exaggeration. Indeed, constitutional law is now firmly settled in this age.”\(^{24}\)

Other critics, whether speaking of the Canadian constitutional system or about other legislative systems around the globe, concur with Webber that “constitutional law is now firmly settled in the age of balancing.”\(^{25}\) For Amir Attaran, “[t]ests over constitutionality are among the most celebrated matches between a person and the state, generating rich public discourse” and the


\(^{22}\) *R v Oakes*, [1986] 1 SCR 103 at para 73, 26 DLR (4th) 200 [*Oakes*].


\(^{24}\) *Ibid* at 179. By way of example, Webber remarks at 179: “Canadian scholar David Beatty maintains that proportionality is an ‘essential, unavoidable part of every constitutional text’ and ‘a universal criterion of constitutionality’; German scholar Robert Alexy, for his part, maintains that balancing ‘is ubiquitous in law’ and that, in the case of constitutional rights, balancing is unavoidable because ‘there is no other rational way in which the reason for the limitation can be put in relation to the constitutional right.’ Though not always versed in the language of constitutional rights scholarship or jurisprudence, even parliamentarians call for ‘balanced’ policies with regards to constitutional rights.”

\(^{25}\) *Ibid* at 201.
“law and the newspapers are full of instances in which two different, conflicting societal interests are being traded off—or balanced—against one another by the courts.”

Ran Hirschl, in his study of “constitutional theocracy,” similarly isolates balancing as a salient characteristic of present day constitutionalism, which requires the weighing of “fundamental democratic governing principles with realities of very large numbers of participants and inputs” and “serious disagreements among participants on values, worldviews, identities, policy goals, and methods.”

In Hirschl’s opinion proportionality, which he describes as “based on judicious balancing of competing claims, rights, and policy considerations,” has become a “prevalent interpretive method” in comparative circles and the “lingua franca of constitutional jurisprudence” in many jurisdictions, including the United States, Canada, Europe, India, New Zealand and South Africa.

Patrick Monahan and Byron Shaw, in a standard text on Canadian constitutional law, flag the “complex and multidimensional nature of the balancing required in Charter cases,” offering that “the Supreme Court has carefully balanced competing interests in difficult cases, so as to arrive at compromise results.”

---


28 Ibid at 80. He also states that, in addition to these countries, balancing “is making its way into the jurisprudence of many higher courts in the developing world, from Latin America to Asia, Africa, and the Middle East” (ibid). Similarly, Alec Stone Sweet and Jud Mathews argue in “Proportionality Balancing and Global Constitutionalism” (2008) 47 Colum J Transnat'l L 72 at 73-4 that proportionality “is today an overarching principle of constitutional adjudication,” that it is has “come to dominate the dockets of constitutional and supreme courts around the world” and that it now “constitutes one of the defining features of global constitutionalism.”


30 Ibid at 472.
When one turns to examine the structural properties of the Charter and the assorted rules and tests developed over the past several decades to facilitate its analysis and application, one encounters this same emphasis on balancing and proportionality. Take, for instance, s. 1, a critical provision anticipating the guarantees catalogued in later sections which at once sets up and is informed by a tension between government policy on the one hand and liberties on the other. Given pride of place at the start of Part I of the Constitution Act, 1982, this framing device serves a singular purpose: to balance the needs of the state against those seeking relief for constitutional injuries. While the phrase “subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society,” in its most basic sense, entails a single comparative step (reasonable versus unreasonable limitation), the celebrated test created by Dickson C.J.C. in R. v. Oakes ups the ante by incorporating such weighing at multiple stages of the s. 1 inquiry. As summarized by Wilson J. in McKinney v. University of Guelph, “this Court's approach to s. 1 of the Charter has emphasized that Charter interpretation is fundamentally about balancing the rights of the citizen against the legitimate objectives of government.”

---

31 Charter, supra note 14 at s. 1.
Oakes test as an effort to “strike a proper balance” between state action and constitutional protections.\(^{33}\)

Much like s. 1, other provisions of the Charter will often entail a balancing of rights and interests across a spectrum of contexts. The requirement in s. 7 that one not be deprived of “life, liberty and security of the person” except “in accordance with the principles of fundamental justice”\(^{34}\) has, for example, been treated in this vein. In Suresh v. Canada (Minister of Citizenship and Immigration), the Supreme Court of Canada acknowledges “the balancing process mandated by s. 7,”\(^{35}\) while the Supreme Court of the Northwest Territories explains in another case decided one year earlier that judging s. 7 claims “involves a balancing exercise between the constitutional rights of the individual and the interests of the state.”\(^{36}\) Following suit, s. 24(2) has also been said to “introduce… a balancing process”\(^{37}\) into the task of ascertaining the status of evidence adduced against persons standing accused of a crime, an adjudicative function calling for a careful analysis of probative versus prejudicial value. Sections 9 and 10 of the Charter too have been presented in this way, as noted by McLachlin C.J.C. and Charron J. in R. v. Suberu:

“defining what constitutes a detention for Charter purposes requires courts to balance individual constitutional rights against the public interest in effective law enforcement.”\(^{38}\) Even s. 35,


\(^{34}\) Charter, supra note 14 at s. 7.


\(^{36}\) Germany (Federal Republic) v Ebke, 2001 NWTSC 17 at para 36, 203 DLR (4th) 415.


insofar as it necessitates the parsing of complex treaty rights between communities and
governments, has been read as including a need for balancing and proportionality.\textsuperscript{39}

Beyond the actual text of the \textit{Charter}, many of the tests designed by the Supreme Court of
Canada to address particular constitutional issues incorporate a balancing component. Aside
from \textit{Oakes}, other well-known formulae have drawn from this pervasive theme and have centred
on proportional weighing. In the freedom of expression context, one obvious example of this
push for balance is the \textit{Dagenais / Mentuck} test developed in response to press challenges to
publication bans imposed in criminal and other proceedings. First formulated in 1994 and later
refined in 2001, this rule, despite significant shifts in emphasis, retains its focus on the weighing
of “salutary” and “deleterious” effects flowing from the ban at issue.\textsuperscript{40} Just as the second branch
of the earlier version comes out against disclosure where the “salutary effects of the publication
ban outweigh the deleterious effects to the free expression of those affected by [it],” a similar
effect is achieved in the next iteration through its unpacking of concepts like freedom of
expression, trial fairness and the administration of justice.\textsuperscript{41} As specified by Iacobucci J. in \textit{R. v.
Mentuck}, this approach forces courts to “balance the interests” of the public, the state and the
accused rather than “enshrining one [right] at the expense of the other.”\textsuperscript{42} According to him, this

\textsuperscript{39} For Monahan and Shaw, s. 35 “requires a careful balancing of interests between Aboriginal
rights and the continuing role of Parliament and the provincial legislatures to advance the
collective interests of society as a whole.” (\textit{supra} note 29 at 27).

\textsuperscript{40} \textit{R v Mentuck}, [2001] 3 SCR 442 at paras 23, 32, 205 DLR (4th) 512. See also \textit{Dagenais v

\textsuperscript{41} \textit{Ibid}.

\textsuperscript{42} \textit{Ibid} at para 23.
solution mimics the “valuable function [of Oakes] in determining what reasonable limits on the rights to be balanced might be.”

Whether reflected in the constituent parts of the Charter or the juridical devices introduced to help give them expression, the “age of balancing” is in full display in Canadian constitutional law, even pre-1982. In one sense such balancing is, as maintained by the above-noted writers, common across many jurisdictions and can be viewed most simply as a natural extension of the concept of justice itself, an ancient trope reflected in the image of scales which adorn many a bar association or other legal organization. On the other hand, it is important to remember that the weighing process at work in Canada is not exactly replicated across other legal systems, even in places with familiar approaches to other kinds of juridical questions. This is especially so with respect to s. 1, a limiting provision without direct correlative in the United States where the dissecting of constitutional problems does not allow the state, once a violation has been identified by a court, to defend this infringement on the basis of a pressing and substantial objective or some other ground. Our balancing culture is home grown, so to speak, and while it may be informed by developments south of the border or elsewhere, it retains a distinctiveness

43 Ibid.
44 Webber, supra note 23 at 179.
45 As observed by L’Heureux-Dubé J. in Committee for the Commonwealth of Canada v Canada, [1991] 1 SCR 139 at para 88, 77 DLR (4th) 385: “The pre-Charter decisions appreciated that rights are not absolute. See e.g. Reference Re Alberta Statutes, supra; Boucher v. The King, supra; Saumur v. City of Quebec… and Switzman v. Elbling, supra. Another example of this recognition can be found in Fraser v. Public Service Staff Relations Board… the last pre-Charter case on freedom of expression.”
46 To cite but one prominent Canadian example, the Canadian Bar Association (and its provincial branches) has adopted this image as its official logo. See online: <http://www.cba.org/Home>.
47 See Attaran, supra note 26, at 269-70.
borne out of a specific vision of constitutionalism promoting, among other things, accommodation and the mediating of competing interests.

2.2 Private lives and public speech

It will come as no surprise, given the above discussion, that judges and others have often portrayed the relationship between privacy and freedom of expression as one of conflict in need of balancing and negotiation. Back through the decades and the centuries, this agonistic model has governed to a large extent the manner in which these rights have been understood, and commentators today continue to promote this dichotomous framework. To return to Barendt’s phrase, this “traditional perspective” on the “clash of rights”\textsuperscript{48} between speech and privacy is alive and well, and still looms large in much of the judicial and other writing on point. For him, the proposition that “privacy rights and interests inevitably conflict with the right to freedom of speech” is a “familiar theme”\textsuperscript{49} in the literature on defamation, press freedom and related themes. As related by Walid Al-Saqaf in his February 11, 2014 post “Privacy vs. Free Speech: Questioning the Conflict” written for the website Advox: “Throughout my years as a journalist, media researcher and activist, I have seen many colleagues envision a dichotomy between privacy and free speech.”\textsuperscript{50} As both Barendt and Al-Saqaf show, the tendency, in the East as well as the West, has been to understand these rights as mutually exclusive and locked in

\textsuperscript{48} Supra note 11 at 11.

\textsuperscript{49} Supra note 11 at 11.

combat, as warring factions struggling on a “battleground on which the competing values of free expression and protection of reputation collide.”

One chief battleground for such conflict is defamation and related press freedom skirmishes, where “constitutional conflicts between privacy and freedom of the press” regularly constitute the legal centre point for argument and debate. As with other scenarios inviting this struggle, the defamation question has long featured this schism between privacy and free speech, often leavened with much hostility toward denizens of the fourth estate accused of privacy invasion (and often worse) to sell a story and score a scoop. In The Right to Privacy, the 1890 Harvard Law Review article written by Samuel Warren and Louis Brandeis and a founding academic text of the privacy movement in the West, this is exactly the tact taken as a sharp line is drawn between one’s personal world and public expression. The authors, responding most immediately to the invention of the instant Kodak camera, eloquently despair that this line is being crossed and that the “press is overstepping in every direction the obvious bounds of propriety and of decency.” Warren and Brandeis, in their demand for the recognition of the “more general right

---

55 Supra note 53 at 195 (“Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life”).
56 Ibid at 196. For them it is the “unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented” (ibid at 215).
of the individual to be let alone”¹⁵⁷ and their rejection of “recent inventions and business methods,”¹⁵⁸ anticipate the myriad technological and other concerns of contemporary privacy advocates. Further, in contending that “gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery,”¹⁵⁹ they capture the tenor of many defamation lawsuits currently being litigated in Canadian courts.

Fast-forward one hundred and twenty something years and critics continue to characterize privacy and freedom of expression in terms of conflict and struggle, though admittedly with less invective and outrage. In Balancing Privacy and Free Speech Mark Tunick presents his twenty-first century version of this argument, explaining in his introduction that “this book addresses the question of how we are to balance privacy and free speech in the age of digital media.”¹⁶⁰ While he is quick to concede that these “two values go hand in hand,”¹⁶¹ his project in the main revolves

---

¹⁵⁷ Ibid at 205. They note: “The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual”(ibid at 196).

¹⁵⁸ Ibid at 195.

¹⁵⁹ Ibid at 196. In a decidedly less polished vein, the Sex Pistols make the same point in “I Wanna Be Me” (EMI Music Publishing Ltd., November 26, 1976, B-side of the “Anarchy in the U.K.” 45 RPM single) when, railing at journalists who had been covering their exploits, they snarl: “I got you in the camera / And I got you in my camera / A second of your life / Ruined for life / You wanna ruin me in your magazine / You wanna cover us in margarine.”

¹⁶⁰ Mark Tunick, Balancing Privacy and Free Speech (New York: Routledge 2015) at 6. Other authors have telescoped these concepts of tension and balancing in the titles of their academic studies. Stefan Braun, in Democracy Off Balance: Freedom of Expression and Hate Propaganda Law in Canada (Toronto: University of Toronto Press, 2004), advises that “the ideas of 'balance' and 'balancing' pervade this book” (at 10). See also The Clash of Rights by Paul Snideman, Joseph F Fletcher, Peter Russell & Philip E Tetlock (New Haven: Yale University Press, 1996), an examination of competing rights in the Canadian context.

¹⁶¹ Ibid at 14. He allows that “there are many circumstances in which free speech is not in conflict with privacy and the two values go hand in hand. Sometimes to be free to communicate one needs to assurance of confidentiality or anonymity.”
around efforts to set out the “philosophical foundations of a balancing approach” and erect a “framework for the balancing privacy and free speech.”

This same emphasis on the tension between expression and privacy is also highlighted in other scholarship across a range of topics. John D. R. Craig, calling for a privacy tort over a decade prior to the creation in Ontario of such a private law remedy, remarks that the fact that Canadian courts do not “recognize a hierarchy of rights” has “placed the judiciary in the position of having to balance the free-speech right of one party with the competing interests advanced by the opposing party.”

Similarly, Wayne MacKay, in his exploration of cyberbullying, speaks of the “central conflicts between privacy and freedom of speech” behind the efforts of victims to push for legislation designed to target this destructive activity.

In Hill v. Church of Scientology of Toronto, a classic statement by the Supreme Court of Canada on defamation and the limits of privacy and free speech, Cory J. opines that “there can be no

---

62 Ibid at 133, 129.
63 Jones, supra note 12.
65 Supra note 52 at 113.
doubt that in libel cases the twin values of reputation and freedom of expression will clash.”

Observing that privacy is intimately connected to reputation and “has been accorded constitutional protection,” he goes on to observe that the “protection of a person's reputation is indeed worthy of protection in our democratic society and must be carefully balanced against the equally important right of freedom of expression.” And again: “Freedom of speech, like any other freedom, is subject to the law and must be balanced against the essential need of the individuals to protect their reputation.” While such statements concern the issue of reputational damage specifically, Cory J. in his introductory remarks on s. 2(b) establishes broadly that “freedom of expression has never been recognized as an absolute right.” In finding for the defamed prosecutor, he at once stresses the low constitutional protection to be accorded to libellous speech but, at the same time, at least suggests the possibility that, even absent libel or slander, one can never fully escape the necessity of balancing speech against privacy (or some other right). The ideas of “conflict” and “limits” are central to this judgment, and Cory J. is transparent in presenting speech as a right to be negotiated in tandem with other interests.

Much the same messaging can be gleaned from other Supreme Court of Canada decisions relating to defamation, press freedom and a host of other topics. In Edmonton Journal v. Alberta

---

67 Supra note 19 at para 100.
68 Ibid at para 121.
69 Ibid at para 138.
70 Ibid at para 102. Interestingly, while many references in the case law to this need for balancing focus on free speech, not privacy, the Court of Appeal for Ontario in Jones, supra note 12, suggests that it is privacy, rather than expression, which is in need of limiting: “Finally, claims for the protection of privacy may give rise to competing claims. Foremost are claims for the protection of freedom of expression and freedom of the press...no right to privacy can be absolute and many claims for the protection of privacy will have to be reconciled with, and even yield to, such competing claims” (para. 73).
71 Ibid at para 103.
(Attorney General), Wilson J. writes in a concurring opinion that, regarding the ability of journalists to report on the private details of marital disputes referenced in court, both free speech and privacy “cannot be fully respected” and promotes a “contextual approach in balancing the right to privacy against freedom of the press under s. 1.” Returning to the central theme of Hill v. Church of Scientology of Toronto, Cory J. in R. v. Lucas reiterates that “unrestricted freedom of expression may interfere with legitimate interests in privacy and reputation” and advises that a “balance must be struck” to resolve matters. That same year, the court in Aubry v. Éditions Vice-Versa tackled a “balancing of the right to privacy and freedom of expression,” and was still some two decades later in Grant finessing its judicial approach to these “conflicting values.” Another recent judgment: Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401, is noteworthy because, unlike the cases just cited, it does not focus on defamation or press freedom. Here the court, writing about the collection and disclosure of personal information during a labour dispute, reaffirms that “like privacy, freedom of expression is not an absolute value and both the nature of the privacy interests implicated and the nature of the expression must be considered in striking an appropriate balance.”

---

72 Edmonton Journal, supra note 18 at para 46.
74 Ibid at para 16.
76 Supra note 10 at para 3.
77 Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401, 2013 SCC 62, [2013] 3 SCR 733 [United Food].
78 Ibid at para 38.
It is reasonable to suspect that, in the coming years, we will with increasing frequency encounter legal challenges to the collection and dissemination of personal information of the sort featured in *United Food*. While the complainants in this case were upset that union organizers had captured their image by means of photography (harkening back, in some sense, to the attack on the nascent Kodak technology central to Warren and Brandeis’ 1890 text), one can assume that emerging online technologies and platforms will provide fertile ground for such arguments over the invasion of privacy and its impact on free speech. As our lives continue to migrate into cyberspace and we reveal–knowingly or otherwise–a steady stream of private details, so too will this collision of rights proliferate, particularly as journalists and others in the speech business seize upon these new troves of personal information. Whereas for Warren, Brandeis and the picket line crossers in *United Food* it is the roving camera which proves offensive, the internet presents many other ways in which data once considered off-limits to the public is suddenly available to strangers at the click of a button. It is important to note, however, that while these new information highways have required a shift in legal thinking, the conceptual logic remains the same: a clash of rights to be solved through a “balancing equation.”

### 2.3 The right to be forgotten

One of the most widely discussed examples of this clash of privacy and freedom of expression on the internet has come to be known as the right to be forgotten, an ability to request a search engine or related entity to delete from cyberspace information which the complainant deems harmful to his or her interests. More often than not, this struggle will arise where a news organization has previously in good faith reported details regarding the complainant and,

---

79 *Lucas, supra* note 73 at para 16.
sometimes many years later, this unflattering or otherwise problematic information continues to exist online for all to see. Unlike newspapers, which fall quickly out of circulation as they are superseded by newer editions and live out their days in archives or forgotten at the back of a closet, journalism published on the web can have a long shelf life and can with facility be unearthed well after the underlying facts have gone stale. Frozen in time, such data, which remains from the perspective of the originating news source credible reporting, may haunt its subject and result in considerable after-shock effects. Even more of an “unwarranted invasion of individual privacy” than the stealthy snapshots excoriated by Warren and Brandeis, this stickiness of data accessed through a computer has important implications for free speech and privacy proponents alike.

The right to be forgotten made headlines in May 2014, when the Court of Justice of the European Union released its decision in *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*. Mr. González, a Spanish national, was seeking to compel both Google and *La Vanguardia*, a Spanish daily newspaper, to remove from the internet two pages from this publication dating back to 1998 that referenced his name in connection with proceedings for the recovery of social security debts. As stated by the court, the complainant was concerned that these proceedings “had been fully resolved for a number of years and that reference to them was now entirely irrelevant.”

---

80 Supra note 53 at 215.
82 Ibid at para 14.
83 Ibid at para 15.
ongoing availability of his personal data online, the court noted (borrowing language from the AEPD, which had upheld the initial complaint against Google but not against *La Vanguardia*) that the “dissemination of the data [is] liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense.”

In this ruling attention is paid to the need for “balance,” not only concerning Mr. González’s rights but also those of internet users generally and “the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.”

In the end, Mr. González was granted a “right to be forgotten” on the basis of articles 7 and 8 of the *Charter of Fundamental Rights of the European Union*, as a result of which Google was forced to scrub his data from its server. This outcome caused a sensation in legal circles, with at least some commentators expressing concern over the negative implications for free speech. As Jeffrey Rosen puts it, this development “represents the biggest threat to free speech on the Internet in the coming decade” and, consequently, “it’s hard to imagine that the internet…will be as free and open as it is now.” While it is true that European approaches to free speech and privacy may well differ from those adopted in the United States in that the first has (as reflected in the González decision) tended to privilege privacy while the second has long been known as a

---

84 *Ibid* at para 17.
85 *Ibid* at para 81.
86 *Ibid* at para 91.
87 Jeffrey Rosen, “The Right to Be Forgotten”, online: (2012) 64 Stan L Rev 88 <http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten>. He concludes: “It’s hard to imagine that the Internet…will be as free and open as it is now.” As Paul Bernal summarizes: “Much of the opposition to the idea of a ‘right to be forgotten' has been based on the idea of it being an infringement on free speech” (*supra* note 66 at 201).
defender of speech,\textsuperscript{88} variants of this license to forget have been introduced in the American context. More than half a year prior to the Court of Justice of the European Union ruling, the Governor of California approved Senate Bill No. 568, more commonly known as the “online erasure law,”\textsuperscript{89} allowing state residents under the age of 18 to have deleted “content or information posted on the operator’s Internet Web site, online service, online application, or mobile application.”\textsuperscript{90} Even in Canada, the impact of such judicial and legislative events is slowly making its mark and might well feature in litigation in the near future.\textsuperscript{91}

Most recently, the European Union is preparing to adopt its \textit{General Data Protection Regulation} (‘GDPR’),\textsuperscript{92} a system of rules planned as a unified code to replace the disparate laws introduced by member states to implement the 1995 Data Protection Directive.\textsuperscript{93} From the perspective of

\textsuperscript{88} James Q Whitman, in “The Two Western Cultures of Privacy: Dignity versus Liberty” (2013) 113 Yale LJ 1151, reflects on this distinction by focusing on what he identifies as competing sensibilities focused on dignity (Europe) versus liberty (United States).


\textsuperscript{90} California Senate Bill No 568, c 336, 22581(a)(1), online: <http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568>. For related U.S. legislative developments at the state and federal level See also Caitlin Dewey, “How the ‘right to be forgotten’ could take over the American Internet, too”, \textit{Washington Post} (4 August 2015), online: <https://www.washingtonpost.com/news/the-intersect/wp/2015/08/04/how-the-right-to-be-forgotten-could-take-over-the-american-internet-too>.

\textsuperscript{91} In \textit{Niemela v Malamas}, 2015 BCSC 1024 the Supreme Court of British Columbia dismissed the plaintiff’s request to block Google search results which, he claimed, were defamatory. For a discussion of the right to be forgotten in the Canadian context see Christopher Berzins, “The Right to Be Forgotten after Google Spain: Is It Coming to Canada?” (2015) 28 Can J Admin L & Prac 267.


\textsuperscript{93} Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free
free speech and privacy experts a key section of the GDPR is article 17, which outlines a “data subject’s right to be forgotten and to erasure.” Among other things, article 17 directs that this erasure shall be available in certain circumstances, including when the “data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.”

This concept of necessity is nowhere defined, and is more than likely to spark litigation down the road as parties endeavour to establish that a collection purpose has or has not expired, as the case may be. In turning to the issue of freedom of expression the GDPR proposal, joining the chorus of courts and commentators endorsing the “traditional perspective” rooted in balance, says that “Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights.”

Beyond creating a massive amount of work for Google, this erasure initiative telescopes, in the most contemporary of ways, the ongoing tension between expression and the private realm.

For speech proponents, this move toward an expansion of the right to be forgotten is most alarming given that it targets speech which, presumably, would pass muster in defamation cases and similar proceedings. Unlike defamatory speech, which is untrue or otherwise problematic in law, speech targeted by this right, generally speaking, is attacked by the plaintiff, at some later date following its original publication, as inconvenient or “irrelevant,” to use the language of the movement of such data, online: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>.

---

94 Supra note 92 at 9.
95 Ibid at 51.
96 Barendt, supra note 11 at 11.
97 Supra note 92 at 35.
Court of Justice of the European Union in González.\textsuperscript{99} Taking this case as an example, the facts at issue: that Mr. González had at some point in the past experienced financial difficulties, are true, a reality never disputed at any point during the litigation. Accordingly, one is confronted here with a more fragile concept of reputation than has heretofore featured in traditional defamation law. While in the latter a plaintiff is required to demonstrate that the expression under scrutiny crosses some established legal line (because, for instance, it is untrue), the right to be forgotten largely does away with these checks and balances. In this emerging context, one is no longer required to pinpoint such line crossing by the defendant – all that is needed is to show how one has moved on in one’s life in a manner at odds with the statement(s) in question. This is a remarkable reversal, and should cause concern among expression advocates and prompt discussion in any jurisdiction seeking to import this regime into its domestic legal system.

At the same time, one can certainly understand this desire to be left alone, or at least some wish to escape the potential permanence which may now accompany internet publication. One can assume that, when La Vanguardia originally published the offensive articles in 1998, Mr. González might not have realized (at the dawn of the Google era\textsuperscript{100}) that they could live online indefinitely. Today, as our lives are pulled further and further in a web spiral, one can appreciate why some individuals would seek to keep at least part of their lives offline. This is particularly so, of course, for someone like Mr. González who was not responsible for the speech he later sought to stifle before the Court of Justice of the European Union. Quite rightfully, in my opinion, Google has resisted requests to remove information initially posted on the internet by

\textsuperscript{99} Supra note 81 at para 15.

\textsuperscript{100} For a history of Google see the timeline provided on its website, online: <https://www.google.com/about/company/history>.
the requester him or herself. While in my view all removal requests should, if not resisted outright, at least be subject to heightened scrutiny, it should I think be especially difficult for the requester to delete expression for which he or she is responsible. If the speech is created by someone else, one can at least suggest that he or she had no control over the expression which is now, it is alleged, causing some hardship or injury beyond the defamation context. That said, shutting down the speech of third parties is censorship, plain and simple (self-authorship requests raise a different issue), a stark reality to which politicians and judges should remain alert.

3 Privacy as a mechanism for freedom of expression

3.1 From clash to continuity of rights

I have, in the preceding pages, sought to outline the extent to which, in historical and contemporary contexts, freedom of expression and privacy have often been construed as incompatible rights in need of balancing. In this section I seek to outline a less traditional but nonetheless vital alternative view of this relationship, pursuant to which the very possibility of speech is facilitated, and at times dependent, on anonymity, one facet of the privacy interest. While it is certainly true, as explained above, that this proportionality metric constitutes the basis for a great deal of the analysis on point, it is not the only framework within which to consider these issues. In a recent study of the privacy landscape in Canada, Graham Mayeda suggests as much, noting the limitations of the “‘balancing rights’ paradigm” and the “‘competing rights’ approach that animates many of our laws, policies and jurisprudence in this area.”


102 Graham Mayeda, "My Neighbour’s Kid Just Bought a Drone ... New Paradigms for Privacy Law in Canada" (2015) 35 NJCL 59 at 60-1.
Mayeda does not focus on free speech or its connection to privacy,¹⁰³ his identification of other lenses through which to understand such matters brings home the availability of other modes of thinking possibly “more suitable” in some instances “for addressing new dimensions of privacy.”¹⁰⁴ This insight is apposite in light of ongoing changes to online culture and our place in it, and provides a useful starting point for my own efforts to track the speech-privacy continuum in this new reality.¹⁰⁵

Barendt, as well as setting forth the “traditional [balancing] perspective” on these rights, underlines that the “protection of privacy is often essential to freedom of speech,” particularly in the “context of electronic communications by the internet,” and that there are “contexts in which privacy and freedom of speech go hand in hand.”¹⁰⁶ Nadine Strossen, likewise, in a paper published while she was President of the American Civil Liberties Union, pauses to reflect on the “continuing positive connections between privacy and free speech,” averring that in “many situations, these two sets of rights are mutually reinforcing,” like the “area of anonymous or

¹⁰³ He focuses rather on what he terms “the idea of privacy as an emergent right” (ibid at 61) though, when he does reference free speech, he emphasizes the way it is caught up in a “balancing approach” promoted by “courts and policy-makers” (ibid at 78).
¹⁰⁴ Ibid at 60.
¹⁰⁵ While privacy and anonymity are not synonymous, they are intertwined concepts, particularly as contemporary notions of privacy remain in flux and continue to shift in response to swift technological change. See Timothy Macklem, Independence of Mind (Oxford, Oxford University Press, 2006) at 61.
¹⁰⁶ Supra note 11 at 11-12. He elaborates: “There is a vast amount of literature both on privacy and on freedom of speech...as discrete constitutional and legal rights...But now the advent of novel electronic technologies for communication gives a fresh impetus to the discussion and invites reconsideration of a familiar theme. Simply stated, this theme is that privacy rights and interests inevitably conflict with the right to freedom of speech” (at 11).
pseudonymous communications, including those communications that take place online.” In arguing thus, Barendt and Strossen hold up this continuity model as a counterpoint to that balancing paradigm at the centre of the case law catalogued in the preceding section of this chapter. Additionally, as they make explicit, such issues have become that much more pressing given the prominence of online culture and the technological impact of this culture shift on privacy and expression. This holds particularly true for anonymity, a state of mind and being facilitated (at times with very negative consequences) through cyberspace which continues to push the frontiers of civil liberties advocacy in Canada and elsewhere.

The purpose of anonymity is to create for the speaker a safe zone in which he or she can express him or herself without fear of reprisal. This sheltering function of privacy, what “prominent champions of free speech rights have viewed,” writes Strossen, as the “ultimate bedrock of all our civil liberties,” is a defining feature of anonymous speech routinely seized upon by critics. For Timothy Macklem, it is “sponsor and guardian to the creative and the subversive,” an “isolating shield” allowing individuals to “develop and exchange ideas…that the presence or even awareness of other people might stifle.” According to Richard A. Spinello the “exercise

107 Supra note 54 at 2105-06. Strossen reminds her audience that “despite specific situations where there is an apparent conflict between free speech and privacy rights, all of us who value free speech have a real stake in preserving a robust privacy right as well” (ibid at 2106).
108 While, as explored in further detail below, online anonymity fosters free speech and other related social goods, it can of course equally facilitate socially destructive conduct, including defamation, cyberbullying and a range of other harmful activities.
110 Supra note 105 at 36.
of freedom and especially free expression does require the support of anonymity in some situations.”\textsuperscript{111} while, for Saskia Sell, this stealth status affords the opportunity to “regain privacy inside the realm of public communication while actively taking part in the negotiation processes of the public sphere.”\textsuperscript{112} Simply put, to cite Saul Levmore, the “great promise of anonymity is that important information or viewpoints might be chilled if authors know they will be identified,”\textsuperscript{113} a reality that has changed little over the years. As Oscar Wilde, always one for the \textit{bon mot}, quips in his 1891 essay \textit{The Critic as Artist}: “Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth.”\textsuperscript{114}

Additionally, beyond merely protecting speech \textit{per se}, privacy allows for space within which one is free to explore and exchange ideas which might at some point result in expression.

Facilitating what might be characterized as pre-expression, this second function of the private sphere is critical to our well-being in creating room for unalloyed thought and creativity. Neil Richards has spoken of this state as “intellectual privacy,” which he characterizes as a “freedom from interference or surveillance when we are engaging in ideas and beliefs” essential, in his

\textsuperscript{111} Richard A Spinello, \textit{Cyberethics: Morality and Law in Cyberspace} (Sudbury, MA: Jones and Bartlett Publishers, 2006) at 74.
\textsuperscript{112} Saskia Sell, “‘We are Anonymous.’ Anonymity in the Public Sphere: Challenges of Free and Open Communication”, online: (2013) 3:1 Global Media J. Germany ed at 4, online: <http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-27642/GMJ5_Sell_final.pdf>.
\textsuperscript{114} Oscar Wilde, “The Critic as Artist” in Richard Ellmann, ed, \textit{The Artist as Critic: Critical Writings of Oscar Wilde} (New York: Random House, 1968) 340 at 389. Note, of course, that the openness and transparency referenced by Wilde concerns freedom of thought as much as it does freedom of expression.
view, to “both free speech and a democratic culture.”115 Section 2(b) of the Charter and similar provisions included in other domestic and international constitutional and human rights instruments protect freedom of thought as well as expression,116 and the cover afforded by online (and other forms of) privacy guarantees opportunities for uninhibited reflection. As it becomes easier to track such pre-speech, however, the likelihood of a chilling effect grows in turn, as the risk of government surveillance instills fear of the exposure of ideas not intended, at least at that stage, for public consumption.117 John Stuart Mill, in his 1859 treatise On Liberty, comments that “ancient commonwealths” sought to enforce the “regulation of every part of private conduct by public authority,”118 and such efforts to map private thinking and experience have only grown more numerous and effective in the years since his publication first shook Victorian England.

It would be erroneous to locate the rise of anonymity as a tool for expression in the immediate present, given that this strategy has been adopted by writers and artists for a very long time. The history of anonymous communication is long and storied, and features some notable successes and failures, including horrific punishments meted out to publishers unlucky enough to be singled out for unattributed writings deemed offensive by a King, Queen or other potentate upset by a specific work.119 As outlined by Alex Kozinski, who offers a broad historical overview of

115 Supra note 11 at 153.
this survival tactic: “anonymity has venerable historical roots in political, religious and social revolutions” and, among other texts, “the Federal Papers and many other Revolution-era pamphlets were circulated anonymously.”\textsuperscript{120} History is rife with examples of the use of this technique by rogues and revolutionaries to promote free speech, and even a cursory review of the relevant scholarship confronts the reader with a plethora of instances where names were withheld to protect an author from censure or worse.\textsuperscript{121} “Anyone interested in literary history will find that anonymity is ubiquitous,”\textsuperscript{122} as John Mullan puts it, and trawling prior decades and centuries for anonymous texts will soon turn up an over-abundance of raw materials for dissection.

There is much evidence confirming that governments of the past (like those of today) were more often than not ill disposed toward this masking of writerly identity, and took legislative and other steps to curb this practice. Well before the advent of Bill C-51 in Canada and similarly privacy-invasive statutes and practices in other jurisdictions, laws were crafted to stop this attempt to speak without being seen. One such response, honed in Early Modern England under monarchs like Henry VIII, Edward VI and Elizabeth I, was the introduction of a formalized licensing regime which forced printers to include the name of the author and the date of printing.\textsuperscript{123} John Milton’s \textit{Aeropagitica},\textsuperscript{124} one of the great polemics on behalf of free speech in the Western

\textsuperscript{120} Alex Kozinski, “The Two Faces of Anonymity” (2015) 43 Cap U L Rev 1 at 7.
\textsuperscript{121} See note 113. For further examples of such scholarship see also Janet Wright Starner & Barbara Howard Traister, eds, \textit{Anonymity in Early Modern England: 'What's In A name?'} (Surrey, UK: Ashgate, 2011) and Robert J Griffin, ed, \textit{The Faces of Anonymity: Anonymous and Pseudonymous Publications from the Sixteenth to the Twentieth Century} (New York: Palgrave MacMillan, 2003).
\textsuperscript{122} \textit{Supra} note 119 at 296.
\textsuperscript{123} \textit{Ibid} at 142-44.
canon, was itself composed as a retort to a law enacted by Parliament in June 1643: the *Ordinance for the Regulating of Printing*, passed to suppress “sundry private Printing Presses in corners” and “the great late abuses and frequent disorders in Printing many false, forged, scandalous, seditious, libellous, and unlicensed Papers.” Remarkably, however, although Milton rages against different parts of the 1643 order, he goes so far as to compliment its authors (in a naked act of self-interest) on a prior decree mandating that “no book be Printed, unlesse the Printers and the Authors name, or at least the Printers be register'd.”

### 3.2 Anonymity, expression and the internet

With the ascendancy of the web and our colonization of cyberspace, anonymity has again taken a front seat in discussions of privacy and free speech. Much like sixteenth and seventeenth century English rulers, governments in the twenty-first century are faced with a surge in anonymous chatter made possible by newer online technologies. The internet is many things, including “a medium for enabling freedom of expression,” and has revolutionized communications with an impact not unlike that of the invention of the printing press. While in 1983 there were only 500 computers with unique Internet Protocol addresses, according to Spinello, by the turn of the year.

---

125 *Ordinance for the Regulating of Printing*, online: <http://www.british-history.ac.uk/noseries/acts-ordinances-interregnum/pp184-186>.

126 *Ibid*.

127 *Supra* note 124 at 569. He writes: “Those which otherwise come forth, if they be found mischievous and libellous, the fire and the executioner will be the timeliest and the most effectuall remedy, that mans prevention can use” (*Ibid*).

128 As MacKay observes: “Much of what happens online takes place anonymously” (*supra* note 52 at 127).

129 Michael Karanicolas, " Understanding the Internet as a Human Right" (2012) 10 CJLT 263 at 282.

130 Kaye asserts that the “Internet has profound value for freedom of opinion and expression, as it magnifies the voice and multiplies the information within reach of everyone who has access to it. Within a brief period, it has become the central global public forum” (at para 11).
century that number was up to 200 million and, by 2005, had climbed to somewhere in the range of 1 billion.\textsuperscript{131} One can safely assume that this number has continued to swell in the last decade, and with this demographic growth has come a huge increase in the number of individuals able to broadcast from the shadows behind their monitor, smartphone or other electronic devices. We are, it has been said, in the midst of a “renaissance of anonymity,”\textsuperscript{132} and legislators and courts have had to keep pace, as best as they are able, with rapid advances on the technological front. From our vantage point in the present day, looking back at the history of anonymity, it is clear that the availability of this technique has “jumped to a new level within the context of new information and communication technologies.”\textsuperscript{133}

And, of course, governments around the globe have taken notice. In the American context, perhaps the largest market for anonymous speech in the world, heightened anxiety around national security has resulted, as Michael Froomkin warns, in a “lurch against anonymity.”\textsuperscript{134} Certain jurisdictions have taken steps to radically curb such speech, as is the case with a controversial May 2014 Russian law forcing any blogger with 3,000 or more daily online visitors to register with the national media watchdog \textit{Roskomnadzor} and comply with a battery of

\textsuperscript{131} Spinello, \textit{supra} note 111 at 31.
\textsuperscript{133} Sell, \textit{supra} note 112 at 9. Karanicolas puts it thus: “The right to freedom of expression, once largely limited to printing, has exploded in a digital world that provides users with an unprecedented megaphone to broadcast their views” (\textit{supra} note 129 at 263).
\textsuperscript{134} Michael Froomkin, "Anonymity and the Law in the United States" in \textit{Identity Trail, supra} note 132, 441 at 441.
requirements, including the disclosure of their full name and contact information. More subtly, perhaps, the efforts of other governments, including Canada through the introduction of Bill C-51, to monitor the private communications of citizens and shut down expression deemed dangerous, also reflects this concern with internet activity taking place in the absence of a named author or source. Like rulers of yore, contemporary politicians continue to negotiate the problem of anonymous speakers, and face significant challenges in their attempts to craft legal and political solutions to this threat. As Michael Karanicolas explains, the importance of this issue “to online debate is not limited to repressive regimes,” and therefore remains a concern for states and their populations north, south, east and west.

As is explored more fully in chapter two, Canada has certainly pulled its weight, so to speak, with respect to surveillance techniques, keeping tabs on international communications deemed suspect as well as, it appears (despite Ottawa’s insistence to the contrary), expression at home. Bill C-51, for instance, also know as the Anti-Terrorism Act, 2015 (“ATA 2015”), is responsible among other things for creating SCISA, a hugely controversial statute which, as discussed below, permits the sharing of personal information among over a hundred different federal agencies. Such monitoring powers, which speak in part to this concern over anonymous or hidden expression, are packaged in Bill C-51 with other tools designed to monitor and suppress speech. Thus, for instance, the scope of SCISA is defined as covering “activity that undermines the

---

136 For a discussion of certain strategies adopted by states to undermine online anonymity see Kaye, supra note 109 at paras 36-46, 49-55.
137 Supra note 129 at 283.
security of Canada,” an overly broad approach likewise reflected in the new *Criminal Code of Canada* offence against the promotion of “terrorism offences in general.” And although Bill C-51 has captured the public imagination, it is important to recall that it is not the first legislative instrument to equip Ottawa with surveillance capabilities. The *ATA 2001*, in certain respects a prototype of Bill C-51, also expanded the government’s reach into private speech and thought. To cite just one example, explored more fully below, its amendments to the *National Defence Act*, currently being challenged by the BCCLA, vested the Canadian Security Intelligence Service (“CSIS”) with the authority to intercept communications deemed contrary to national security interests.

The truly global nature of this potential challenge to anonymity and freedom of expression is made clear in a May 2015 annual report penned by David Kaye, the United National Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. In his text, presented at the twenty-ninth session of the United Nations Human Rights Council, Kaye stresses both the critical function played by anonymous speech in online communication and the variety of ways in which governments have sought to limit such speech. He avows:

“Anonymity has been recognized for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation and debate.” As proof of the centrality of this role, Kaye recounts that while the phrase “anonymity is not permitted” was initially proposed for inclusion in article 19(1) the *International Covenant on Civil and Political

---

138 *SCISA*, s 2.
139 *Criminal Code of Canada*, RSC, 1985, c C-46, s 83.221(1) [*Criminal Code*].
140 *Supra* note 109.
141 *Ibid* at para 47.
Rights ("ICCPR"), this notion was later rejected on the grounds that “anonymity might at times be necessary to protect the author.”142 In Kaye’s opinion, because this evasion tactic “facilitates opinion and expression in significant ways online, States should protect it and generally not restrict the technologies that provide it.”143 Accordingly, his concluding recommendations call for the championing of encryption and related technology,144 all in the service of shielding our civil liberties from the prying eyes of our political masters.

More so perhaps than any United Nations report or similarly official document, however, the most vivid illustration of the online mash-up of privacy and freedom of expression is the nameless rogue hacker and, in particular, the emergence of the hacktivist group Anonymous. Just as the ongoing debate over the right to be forgotten crystallizes the balancing paradigm examined in the preceding section of this chapter, so too does Anonymous literally embody the intersection of these rights in cyberspace. Announcing anonymity through its name and iconography (a Guy Fawkes mask and an image of a headless man with a question mark for a head),145 this loose collective146 of activists, pranksters and their supporters has become, paradoxically, the public face of this fusion of hidden identity and, to a lesser or greater degree depending on the exploit at issue, free speech. Although it is true that at least some of the

---

142 Ibid.
143 Ibid.
144 Ibid at paras 56-63.
145 See Rob Walker, “Recognizably Anonymous: How did a hacker group that rejects definition develop such a strong visual brand?”, Slate (8 December 2011), online: <http://www.slate.com/articles/arts/design/2011/12/guy_fawkes_mask_how_anonymous_hacker_group_created_a_powerful_visual_brand.html>.
activities attributed to Anonymous have had nothing to do with civil liberties, some of their campaigns, especially more recently, have exhibited a commitment to such principles. Gabriella Coleman, in her anthropological study of Anonymous, pinpoints this defining characteristic, writing that since it is a “by-product of the Internet, it is unsurprising that Anonymous rises up most forcefully and shores up most support when defending values associated with this global communication platform, like free speech.” As a participant is said to have told her in this regard: “Free speech is non-negotiable.”

Under the banner of this “anti-persona,” unidentified hackers have, with a great amount of press attention and hutzpah, taken on Scientology, Fortune 500 corporations and governments, at times seizing upon an explicit freedom of expression mantra. Thus, for instance, in #OpTunisia, an operation in which members succeeded in temporarily disabling several Tunisian state websites in early 2011, the accompanying public statement was larded with references to “free speech” and attempts by President Ben Ali to impose “an outrageous

---

147 See, for instance, Coleman, *ibid* at 30-1; Tom Sorell, “Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous” (2015) 7:3 J of Human Rights Practice 391 at 392, 407; and Danielle Keats Citron, "Civil Rights in Our Information Age" in *Offensive Internet, supra* note 113, 31 at 35. Note that the two tactics most closely associated with Anonymous: doxing (publishing personal information online) and DDoSIng (disabling websites by flooding them with internet traffic), are themselves antithetical to privacy and free speech respectively. Coleman picks up on this irony, quoting a member on the latter: “i dont think DDos can be in the name of freedom of speech…cause it is an act of silencing” (at 133) and recounting in terms of the former that, prior to a media interview, she “dreaded the prospect of being asked about the blatant privacy violations committed by such hacks, and the gymnastics required to explain the use of such tactics by a collective that ostensibly fought to protect privacy” (at 306-7).

148 *Supra* note 146 at 16.
150 Stryker, *supra* note 146 at 15.
151 See chapter 2 of Coleman, *supra* note 146.
153 See the analysis of #OpTunisia which follows.
level of censorship” and block the sites of “dissident bloggers.” Likewise, in Operation Anti-Security or #AntiSec, a series of hacking activities commenced later that same year, Anonymous (working in conjunction with other hacker groups) turned its sights on an assortment of public and private entities which, it was explained, were complicit in online censorship. As trumpeted in a June 2011 announcement on the website Pastebin.com, the purpose of this venture was at least threefold: “immediate and unremitting war” on “freedom-snatching” agents, the defence of “privacy” and the obliteration of those who “try to censor our progress.” Thus pairing privacy and expressive freedom, initiatives like #OpTunisia and #AntiSec, and Anonymous itself, reflect a playful, culturally popular version of that alternative conception of these rights elucidated by Strossen, Barendt and others.

4 Spencer and the privacy-speech continuum
4.1 Introduction to Spencer decision

Given this strong connection between privacy, anonymity and online speech, the time is ripe for more robust constitutional protections in Canada against government incursions into the domain of private internet activity. As a society we are spending increasing amounts of time in cyberspace, and this inescapable fact of modern life should be reflected, one could argue, in those laws created to govern expression and other daily tasks subject to this internet creep. Paul Bernal strikes this note when he posits that, because “the internet is now part of almost every aspect of our lives, from the personal and intimate to the professional,” “privacy on the internet

154 Coleman, supra note 146 at 153. This position is repeated in a letter, sent directly to the Tunisian government, which intones: “You have unilaterally declared war on free speech, democracy, and even your own people” (ibid at 163).
155 See chapter 9 of Coleman, supra note 146.
has never mattered more.”157 That said, with the rising need for privacy has come threats to the private sphere in equal measure, as “online media and [the] rising tide of digital surveillance”158 have rendered it that much harder for individuals to remain, in some cases at least, below the radar. In light of existing and emerging threats of this type (some of which will likely not be discovered until the next Snowden-like leak) and the privacy-speech continuum detailed above, it seems reasonable to probe the possibility of expanding current laws on freedom of expression to more fully reckon with such issues. Canadian courts have recognized the right to informational privacy159 – it makes sense to more fully locate this concept, along with our diurnal routines, online.

And, although it may be true that, for many with no known political affiliation or connections with advocacy groups, this type of privacy invasion remains theoretical, for some it presents a real threat impinging on their speech and thought, particularly online. This point was brought home in a 1998 Charter challenge by the CCLA (reviewed in chapter two) to provisions of the Canadian Security Intelligence Service Act (“CSIS Act”), granting CSIS wide-ranging powers of surveillance relating to “threats to the security of Canada.”160 While this litigation was

157 Supra note 66 at ix. While I focus here on distinctions between private and public activity in the online context, I certainly recognize that ongoing technological changes have complicated such distinctions. Errol P Mendes, in “Democracy, Human Rights and the New Information Technologies in the 21st Century – The Law and Justice of Proportionality and Consensual Alliances” (1999) 10 NJCL 351 at 352, makes this point when he writes: “The new information technologies are breaking down the realms of what is private and what is public… Web sites, discussion groups, electronic commerce and many other forms of information gathering, dissemination and communication, are both private and globally public.”


159 Cromwell J. underlines this point in Spencer, supra note 1, at para 35.

160 Canadian Security Intelligence Service Act, RSC, 1985, c C-23 ss 2, 12.1.
ultimately unsuccessful, given most critically the absence of a proper evidentiary record, Abella J.A, dissenting, underlines the merits of the CCLA’s claim regarding the chilling effects of government snooping. According to her, the “information contained in the 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 C.S.I.S. Act.”\textsuperscript{161} Further, she confirms that, especially for high profile advocacy groups like the CCLA, government surveillance can have actual consequences sufficient to trigger s. 2(b): “There is no question that the perception of C.S.I.S. intervention was, to say the least, unsettling to the people involved and potentially inhibiting.”\textsuperscript{162} What is needed, then, is an effective constitutional remedy for this problem, should such a Charter violation arise.

\textit{Spencer} represents a significant step in this regard. In this case the court was required, for the purpose of the s. 8 test, to determine whether the appellant possessed a reasonable expectation of privacy in his internet subscriber information connected to a particular Internet Protocol address obtained by police in their investigation of child pornography activities.\textsuperscript{163} The court, on the basis of a wide-ranging analysis, concluded that he did have a reasonable expectation of privacy in such information which had, it was further held, been obtained by way of an unlawful search.\textsuperscript{164} While ultimately ruling the evidence to be admissible under s. 24(2),\textsuperscript{165} it is in his approach to the privacy and anonymity principles at the heart of this litigation that Cromwell J., I suggest, pushes the jurisprudence forward with significant implications for freedom of

\begin{flushleft}
\footnotesize
\textsuperscript{161} \textit{Ibid} at para 103. \\
\textsuperscript{162} \textit{Ibid}. \\
\textsuperscript{163} \textit{Ibid} at paras 2, 16. \\
\textsuperscript{164} \textit{Ibid} at paras 66, 74. \\
\textsuperscript{165} \textit{Ibid} at para 81.
\end{flushleft}
expression as well as search and seizure. One could argue that, in addition to the landmark finding that the “right to privacy protected by s. 8 of the Charter ought to be expanded to include online anonymity,” Spencer advances the law in the s. 2(b) constitutional arena. As I propose in this closing section of this chapter, this 2014 decision is instrumental in broadening the ambit of relevant free speech concepts beyond those set out in several lower court judgments concerning online defamation and earlier Supreme Court of Canada proceedings which glance at the interconnectedness of expression and privacy.

Central to Spencer is an insightful analysis of the right to informational privacy, one of three branches of privacy (along with territorial and personal) articulated by the Supreme Court of Canada. In drilling further down into this particular branch, Cromwell J. outlines “at least three conceptually distinct although overlapping understandings of what privacy is…privacy as secrecy, privacy as control and privacy as anonymity.” Cromwell J., in turning his attention to issues of anonymity, is quick to observe that this concept “is not novel” and that “it is particularly important in the context of Internet usage.” Significantly, he repeats this last point almost verbatim a few paragraphs later: “Recognizing that anonymity is one conception of informational privacy seems to me to be particularly important in the context of Internet

---

166 Mayeda, supra note 102 at 66. For a recent analysis of the importance of Spencer in connection with anonymity and search and seizure principles see Hunt and Rankin, supra note 113, where the authors argue that Cromwell J.’s decision “is likely to have a significant, and possibly transformative, impact on section 8 jurisprudence” (at 195).
167 Spencer, supra note 1 at para 35.
168 Ibid at para 38.
169 Ibid at paras 41-2.
usage.”

By means of such repetition, Cromwell J. alerts his audience to a key principle stemming from this case: that online anonymity matters and should be vigorously defended, at least in some situations involving state action. Taking notice of the fact that the internet “has exponentially increased both the quality and quantity of information that is stored about…users,” and advising that users “cannot fully control or even necessarily be aware of who may observe a patter of online activity,” he crafts a Charter remedy responsive to this contemporary reality.

While Cromwell J. might relate that “the notion of privacy as anonymity is not novel,” what he does with this notion, on the other hand, is remarkable not only for privacy and search and seizure law but, equally, for what it accomplishes on s. 2(b) terrain. Quoting A. F. Westin’s Privacy and Freedom, a volume previously relied upon by the Supreme Court of Canada, he singles out “one form of anonymity” where one “wants to present ideas publicly but does not want to be identified as their author.” As Cromwell J. sees it, here “Westin, publishing in 1970, anticipates precisely one of the defining characteristics of some types of Internet communication,” which is “accessible to millions” but not “identified with its author.” In this sweep of the pen (or, more likely, touch of the keystroke), Cromwell J. explicitly incorporates into his judgment that alternative vision of privacy and free speech as complimentary rights

---

170 Ibid at para 45. Later in the decision Cromwell J. essentially repeats this principle a third time, observing that Doherty J.A. concluded in R v Ward, 2012 ONCA 660, 112 OR (3d) 321 that “some degree of anonymity is a feature of much Internet activity” (ibid at para 48) [Ward].
171 Ibid at para 46.
172 Ibid at para 42.
174 Supra note 1 at para 45.
175 Ibid.
surveyed in the preceding section of this chapter. *Spencer*, skirting around that largely unbroken judicial tradition of pitting these interests against one another, breaks new ground by tracing points of intersection linking privacy and expression in cyberspace. Only five years or so ago it could reasonably have been written that in “Canada, there is no general right to anonymity” and that the role of such a right in “facilitating the exercise of [speech] has not been established”\(^{176}\) This case, I propose, goes a long way toward rectify this legal blind spot.

As a side note, it is interesting to observe that while Cromwell J.’s notions of privacy, speech and defamation are anchored in Westin’s 1970 text, his conclusions on point are also decidedly modern in emphasizing the exponential growth of user information captured online. Although he certainly does glance backward in confirming that the “notion of privacy as anonymity is not novel,”\(^{177}\) he forcefully locates his reasons in the present by stressing this inescapable fact of modern living. He states: “the Internet has exponentially increased both the quality and quantity of information that is stored about Internet users. Browsing logs, for example, may provide detailed information about users’ interests. Search engines may gather records of users’ search terms.”\(^{178}\) Relating the myriad ways in which “advertisers may track their users across networks of websites” and the deployment of “cookies…to track consumer habits,”\(^{179}\) Cromwell J. suggests the many perils (government and corporate) of contemporary internet use. In this grave new world, he relates, the “user cannot fully control or even necessarily be aware of who may observe a pattern of online activity,” a problem which can be remedied “by remaining


\(^{177}\) *Supra* note 1 at para 42.

\(^{178}\) *Ibid* at para 46.

\(^{179}\) *Ibid*. 
anonymous” and thus “assur[ing] that the activity remains private.”\textsuperscript{180} While articulated in a s. 8 context, this rationale for anonymity is likewise germane to s. 2(b), particularly at this historical moment when, as Cromwell J., suggests, our online data trail is being tracked by multiple actors.

4.2 \textit{Spencer advances case law concerning privacy and speech}

It is true that Canadian courts, particularly in the emerging online defamation context, have already referenced (and continue to elaborate upon) the essential role played by privacy, and anonymity in particular, in the promotion of s. 2(b) values. Thus in \textit{Warman v. Wilkins-Fournier}, a 2010 ruling of the Divisional Court of the Ontario Superior Court of Justice involving attempts by the plaintiff to unmask the identities of several John Doe defendants accused of defaming him, the court accepts that there is “support in the case law for the proposition that the removal of an individual's right to remain anonymous may constitute an unjustified breach of freedom of expression.”\textsuperscript{181} Noting that the “right to publish anonymously is a well established aspect of freedom of speech protected by the First Amendment”\textsuperscript{182} Wilton-Siegel J. finds that hindering online anonymity in Canada may likewise impair the s. 2(b) guarantee. Much the same approach informs \textit{King v. Power},\textsuperscript{183} another internet defamation case decided by the Newfoundland and Labrador Superior Court in 2015. Goodridge J., relying on \textit{Warman},\textsuperscript{184} concurs with Wilton-Siegel J. that the “issues of privacy and free expression associated with anonymous use of the internet engage [the] \textit{Canadian Charter of Rights and

\begin{footnotesize}
\begin{enumerate}
\item[Ibid.]\textsuperscript{180}
\item[\textit{Warman v Wilkins-Fournier}, 2010 ONSC 2126 at para 17, 100 OR (3d) 648 (Div Ct) [\textit{Warman}].]\textsuperscript{181}
\item[Ibid.]\textsuperscript{182}
\item[\textit{King v Power}, 2015 NLTD(G) 32, [2015] NJ No 78 (QL) [\textit{King}].]\textsuperscript{183}
\item[Ibid at para 19-20.]\textsuperscript{184}
\end{enumerate}
\end{footnotesize}
“Freedoms.” Further, he reasons that “disclosure cannot be automatic where Charter values are engaged” as the “interests of privacy and free expression would need to be considered and then weighed against the public interest in disclosure.”

As well, the Supreme Court of Canada has itself previously raised the possibility that privacy could be characterized as a vehicle, not an obstacle, for freedom of expression. Over twenty five years ago the court, in Canada (Human Rights Commission) v. Taylor, floated such a possibility in its discussion of hate speech and s. 13(1) of the Canadian Human Rights Act. Contrasting this section, which “works to suppress private communications,” with s. 319(2) of the Criminal Code, which includes a carve-out for “private conversation” that “wilfully promotes hatred,” Dickson C.J.C. reflects on this significant difference and the fact that the “connection between s. 2(b) and privacy is thus not to be rashly dismissed.” Just over a decade later, in R. v. Sharpe, McLachlin C.J.C. revisits the speech-privacy continuum in relation to child pornography, in the course of which she reflects that the “private nature of the proscribed material may heighten the seriousness of a limit on free expression.” Asserting that privacy, “while not expressly protected by the Charter,” is nonetheless central to ss. 7 and 8, she

---

185 *Ibid* at para 17.
186 *Ibid*. Both of these decisions, while presenting privacy as a vehicle for free speech, do so in the course of seeking to establish “an appropriate balance between the public interest in favour of disclosure and legitimate interests of privacy and freedom of expression” (*Warman, supra* note 181 at para. 42).
187 *Canada (Human Rights Commission) v Taylor*, [1990] 3 SCR 892, 75 DLR (4th) 577 [Taylor].
188 *Ibid* at para 76.
189 Criminal Code, s 319(2). Note that the terrorism promotion provision at s 83.221 (1) of the Criminal Code, ushered in by Bill C-51, also does not contain a carve-out for private communications.
continues (citing Taylor) that it “may also enhance freedom of expression claims under s. 2(b) of the Charter, for example in the case of hate literature.”\(^{192}\) For her, the “enhancement in the case of hate literature occurs in part because private material may do less harm than public, and in part because the freedoms of conscience, thought and belief are particularly engaged in the private setting.”\(^{193}\)

Sharpe, it should be observed, is also significant in this context for underlining a related point with respect to the intersection of expression and privacy. While much of the analysis relating to s. 2(b) concerns expression, this constitutional provision applies equally to freedom of thought, a concept which I address in greater detail in part three of chapter two. In addition to the anonymity attached to speech, McLachlin C.J.C. makes clear that thought is also protected under s. 2(b), as reflected in her carving out of child pornography exemptions from s. 163.1(4) of the Criminal Code. She states: “The fact remains…that the law may also capture the possession of material that one would not normally think of as ‘child pornography’ and that raises little or no risk of harm to children.”\(^{194}\) Not unlike anonymous speech, the “intensely private, expressive nature of these materials deeply implicates s. 2(b) freedoms, engaging the values of self-fulfilment and self-actualization and engaging the inherent dignity of the individual.”\(^{195}\) As McLachlin C.J.C. asserts, the “restriction imposed by s. 163.1(4) regulates expression where it borders on thought. Indeed, it is a fine line that separates a state attempt to control the private possession of self-created expressive materials from a state attempt to control thought or

\(^{192}\) Ibid.

\(^{193}\) Ibid.

\(^{194}\) Ibid at para 99.

\(^{195}\) Ibid at para 107.
opinion…To ban the possession of our own private musings thus falls perilously close to criminalizing the mere articulation of thought”196 (emphasis added).

Spencer sits apart from these online defamation and earlier Supreme Court of Canada rulings in ways which, I suggest, create a novel precedent in the s. 2(b) framework. Regarding the former, these are not appellate (let alone Supreme Court of Canada) judgments and, while widely known, are not binding on provincial appellate or any federal courts. Further, although they do focus on the right to speak online without self-identification, they (i) are somewhat narrow in their thematic focus and, more significantly, (ii) do not address that notion of pre-speech “intellectual privacy”197 so central to s. 2(b). With respect to Taylor and Sharpe, these decisions, while milestones in and of themselves, do not situate the linking of privacy and freedom of expression within the broader canvas of online culture (despite the fact that Sharpe involves pornography seized from a computer and does mention the dangers posed by the internet for the production and dissemination of such materials198). Also, their treatment of this intersection is tied to a sense of inwardness or erecting boundaries between the impugned speech and the rest of the world, as in the example of the private hate speech tolerated under s. 319(2) of the Criminal Code. This is exactly the opposite of that outward facing, public expression outlined by Cromwell J.: “claimed by [one] who wants to present ideas publicly but does not want to be identified as its author” and “accessible to millions.”199

196 Ibid at para 108. L’Heureux-Dubé, Gonthier and Bastarache JJ., writing in dissent, pick up on this theme in rejecting the s 163.1(4) exceptions carved out by McLachlin C.J.C.: “In our view, the inclusion of written materials in the offence of possession does not amount to thought control” (at para 221).
197 Richards, supra note 11.
198 Sharpe, supra note 190 at para 166.
199 Supra note 1 at para 45.
I suggest that, while this bridging of free speech and privacy in *Spencer* opens up new vistas for s. 8, a helpful next step in developing Cromwell J.’s analysis should include importing this speech *qua* privacy paradigm into s. 2(b). Recognizing government breaches of our privacy as a s. 2(b) problem would only enhance our legal toolkit in the face of this invasive snooping and could prove helpful on a number of fronts. Needless to say, this proposal would need to be justified on various grounds, not least of which is its value added to existing privacy protection devices like ss. 7 and 8 of the *Charter* and the growing field of privacy torts.

While a full accounting of this value is beyond the scope of this chapter, and is addressed more fully in chapter two (particularly in terms of ss. 7 and 8), I offer a few remarks on point. With respect to available torts, these are narrowly tailored and concern themes largely unconnected to the state behaviour at issue here. Much the same could be said of s. 7, which has thus far been limited in its application to privacy to situations arguably ill-suited to such surveillance. Section 2(b) is also preferable to s. 8 for at least two reasons: the elimination of the onerous reasonable

---

200 This expansion of the privacy tort universe continues in Ontario where, several years after *Jones, supra* note 12, which created the tort of intrusion upon seclusion, in 2016 the Ontario Superior Court of Justice in *Jane Doe 464533 v ND*, 2016 ONSC 541 (a case involving what is commonly known as revenge porn) followed suit by recognizing the tort of public disclosure of private facts.

201 Unlike s. 8, which incorporates an explicit privacy component, the language of s. 7 does not include any such reference, and privacy principles have accordingly been read into the “life, liberty and security of the person” guarantee on a case by case basis. In this context, privacy has for instance been said to encompass human dignity *B (R) v Children's Aid Society of Metropolitan Toronto*, [1995] 1 SCR 315 at paras. 80-1, 122 DLR (4th) 1 [Children’s Aid]] and the disclosure of medical records (*R v O’Connor*, [1995] 4 SCR 411 at para 119, 130 DLR (4th) 235 [O’Connor]). Note, however, that such efforts to formally expand s. 7 have met with at least some resistance, as made clear by Bastarache J. in *Blencoe v British Columbia (Human Rights Commission)*, 2000 SCC 44 at paras. 79-80, 97, [2000] 2 SCR 307. Additionally, this s. 7 version of privacy had had little if any play in connection with allegations of censorship of any sort (including speech suppression arising from government surveillance).
expectation of privacy test and, more generally, its underlining that the concept of privacy is broader than this test and encompasses other interests, including speech. Finally, it goes without saying that s. 2(b), given its primary focus on expression, is an obvious choice for any challenge alleging speech (or pre-speech) infringements.

While Canadian courts have not said much regarding this possibility of introducing a privacy component into s. 2(b), this approach is evinced in a lawsuit commenced by the CCLA and Canadian Journalists for Free Expression (“CJFE”) in 2015 in response to Bill C-51. As articulated in the Notice of Application, the information sharing elements of SCISA are impugned on s. 2(b) grounds for imposing a “chill [on] expression and association rights.” As well as attacking such provisions on the basis of s. 7 (the phrase “activity that undermines the security of Canada” is “unconstitutionally vague”) and s. 8, the applicants plead free speech as a further plank in their argument (a tactic also employed by the BCCLA in a similar challenge to the National Defence Act). Here, in effect, the litigants have relied on s. 2(b) in at least two ways: in a more traditional attack on overbroad language (“terrorism offences in general”) said to cast too wide a net over speech, and in challenging the chilling effect on pre-speech (“will deter legitimate expression”) of the “secret” sharing of personal information across

---

202 As discussed in part four of chapter two, the concept of a reasonable expectation of privacy has grown more complex in recent years, particularly in light of the online disclosure of personal information.
204 Ibid at paras. 33, 37.
205 A fuller account of the CCLA/CJFE and BCCLA proceedings is provided in chapter two.
207 Ibid at para. 34.
208 Ibid at para. 35.
government. Despite the fact that the fates of Bill C-51 and this ongoing court case remain unclear with the arrival of Prime Minister Trudeau in Ottawa, this focus on continuity, not conflict, signals the real world application of the privacy-free speech continuum in contemporary Charter litigation.

5 Conclusion

As recent developments in society and law make evident, the need to protect expression in response to privacy breaches continues to make news. Take, for instance, the cause célèbre refusal of Tim Cook, the CEO of Apple, to comply with a court order to create new software designed to bypass existing iPhone security to assist the FBI in an ongoing terrorist investigation. In a February 16, 2016 “customer letter” published on the Apple website, Cook defended this decision in part on the basis that taking those steps demanded by the government, after having cooperated with earlier data requests and “valid subpoenas and search warrants,” would significantly “undermine the very freedoms and liberty our government is meant to protect.” Cook, in addition to making the pitch that reworking the Apple software would expose users to a greater risk of attack by “sophisticated hackers and cybercriminals,” simultaneously raises the spectre that any such “breach of privacy” could also have a “chilling” effect (by, among other things, allowing the state to intercept messages and even access the iPhone microphone and camera) resulting in a form of pre-censorship. As Cook declares, our “freedoms and liberty” are in some sense a function of the private sphere, and constitutional efforts must be made to

---

210 Ibid.
211 Ibid.
ensure that this speech-privacy matrix is acknowledged and protected, particularly given our total immersion in life online.

Although this particular skirmish seems to have been resolved – the authorities were able to hack the iPhone without any assistance from Apple212 – there is little doubt that free speech issues arising from privacy threats will continue to make headlines and, in the process of doing so, to make law. The findings of Cromwell J. in *Spencer* on the facilitative nature of privacy in fostering freedom of expression will, I suggest, prove critical in this regard, and offer fertile ground for future efforts by lawyers and judges to build upon and extend his linking of these rights. As I have proposed, incorporating a privacy component directly within s. 2(b), rather than allowing it to remain within the province of ss. 7 and 8, could add yet another arrow in the quiver of advocates seeking to challenge intrusive government action. More choice is hardly ever a bad thing, and this supplementing of the current privacy repertoire in Canadian constitutional law (and the limitations and hurdles associated with ss. 7 and 8), would only enhance the options available to those engaged in this struggle. Like the evolution of online and other tracking technologies marshalled by the state, so too will legal responses to this monitoring evolve. *Spencer* has opened the door to an innovative means of countering such intrusions, and passing through this threshold holds much promise for the dual liberties of thought and speech enshrined in s. 2(b).

---

In the second half of the thesis I build upon themes outlined in this chapter: the continuity of speech and expression and the use of s. 2(b) as a means of challenging government violations of privacy, particularly online, on constitutional grounds. Taking *Spencer, Taylor, Sharpe* and other cases as starting points, I argue that (i) Canadian law already recognizes this intersection of these two rights and that (ii) such judicial recognition, and a host of other factors, should be leveraged by advocates in pleading s. 2(b) in response to Bill C-51 and similar legislative instruments at the disposal of the federal government. That this approach to s. 2(b) reflects a logical extension of Cromwell J.’s finding in *Spencer* is, I suggest, confirmed in various ways. First, I explore the ongoing lack of clarity regarding the very definition of privacy among legal scholars, a fact which facilitates a privacy-centric reading of s. 2(b). Second, I underscore the way in which courts have insisted on a broad interpretation of s. 2(b) (in addition to their affirming of the privacy-speech nexus) and the rarely noted fact that, in early 1981, Parliamentarians nearly succeeded in introducing a stand alone *Charter* right: the proposed s. 2(e). Finally, I examine how this approach to s. 2(b) is currently featured in constitutional challenges to surveillance-focused national security laws initiated by the CCLA and the BCCLA.

Through such analysis I hope to show how s. 2(b) is informed – thematically and structurally – by privacy concerns and constitutes a useful and unique addition to existing constitutional tools useful in combatting government surveillance. While *Spencer* is groundbreaking in its own right, one can suggest that it does not go far enough in establishing the functionality of s. 2(b) in this privacy context. The most obvious reason for this, as pointed out above, is the simple fact that this litigation, from trial through to the Supreme Court of Canada, remained a s. 8 case at every stage of its development, despite its focus on anonymity principles. Accordingly, I attempt
in chapter two to pick up where *Spencer* leaves off, importing the insights of this seminal case and related decisions into the arena of freedom of expression and thought. It appears that little analysis of this topic has been undertaken to date, and I hope in the second half of this thesis to contribute to this discussion by shedding light on the utility of *Spencer* in this regard. More specifically, I demonstrate in the remainder of this study how Cromwell J.’s analysis facilitates the use of s. 2(b) in the fight against the privacy invasive tendencies of Bill C-51 and similar legislation. In doing so, I cover historical, practical and theoretical ground (by referencing, among other things, Hansard records, recent court pleadings and scholarly studies), in an attempt to furnish as complete a picture as possible of these complex and topical issues.
CHAPTER 2
ONLINE PRIVACY AND THE STRUGGLE FOR EXPRESSION AND THOUGHT

1 Introduction

Everyone has surveillance on the brain these days, judging from the near ubiquity of academic and non-academic writing and popular sentiment which has been devoted to this topic in recent years, particularly post-Snowden. Everywhere one turns, one is confronted with warnings regarding the contemporary dangers of government intrusion (often with the help of a coopted corporate sector), especially online, into the nether regions of our personal lives. According to Neil Richards, we now face a “digital privacy Armageddon,” a political and technological tipping point threatening to explode 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,” a state of affairs which has spawned a cottage industry of “how to” and DIY guides and other materials on anti-surveillance techniques. Laura Poitras, for instance, the documentary filmmaker 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. The Electronic Frontier Foundation, in a similar vein, has prepared “survival” resources for professional journalists and the general public, including “Ten Steps You Can Take Right Now

---

214 Ibid.
Against Internet Surveillance”216 and its web-based “Surveillance Self-Defense” project, described as “Tips, Tools and How-tos for Safer Online Communication.”217

This heightened concern is understandable, particularly in light of the 2013 Snowden revelations and ongoing debates regarding the legality of government incursions into internet privacy and our right to be left alone. Roused by such state interference, and intent on identifying and championing the multiple constitutional rights and interests breached in Canada and elsewhere as a function of this stealth tracking of our online activity, legal experts and non-specialists alike have sparked a “global push back against surveillance.”218 Focused on “law reform, including substantive statutory changes, the overturning of problematic constitutional doctrines, and improved oversight,”219 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 “however privacy may have conceived in times past, today it is tightly tied to


218 Lisa M Austin, “Enough about Me: Why Privacy Is About Power, not Consent (or Harm)” in Austin Sarat, ed, A World Without Privacy (Cambridge: Cambridge University Press, 2015) 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).

219 Ibid.
avoiding surveillance.” For Lyon, who penned this insight over two decades ago, the relentless electronic monitoring of our personal activities by government and corporate actors is the hallmark of the “surveillance society.” Once relegated to the province of paranoids and conspiracy theorists, this Orwellian construct of the Big Brother state has returned with a vengeance since first being coined in 1949 and informs much of the current thinking about privacy and the web.

In Canada, the flashpoint for such concern has been Bill C-51, the omnibus legislation which as is well known introduced new laws and amended existing statutes in ways which could be said to undermine privacy and other rights and interests. One of the centrepieces of this suite of legislative changes is SCISA, which affords Parliament the ability to collect, rely upon 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

---

220 David Lyon, *Electronic Eye: The Rise of Surveillance Society* (Minneapolis, MN: University of Minnesota Press, 1994) at 180. Lyon, a sociologist at Queen’s University in Kingston, Ontario, is alive to these concerns in Canada, relating that as a group Canadians “are very concerned about their privacy” (*ibid*).
221 *Ibid* at 3.
222 Beetson 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” (*supra* note 217). Valerie Steeves, writing in the early days of cyberspace, anticipates this cultural development in “Humanizing Cyberspace: Privacy, Freedom of Speech, and the Information Highway” (1995) 28 Human Rights Research & Education Bull 1, in conjuring “images of an Orwellian future where Big Brother watches from every television screen and computer monitor” (at 5).
224 *SCISA*, ss 3, 5-8, schedule 3.
undermines the security of Canada”\textsuperscript{225} and “terrorism offences in general,”\textsuperscript{226} showcase just some of the fatal flaws critics have identified in the \textit{ATA 2015}.\textsuperscript{227} And, in response to this government offensive on our privacy, Canadians continue to demand transparency and safeguards. As Michael Geist observes: “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.”\textsuperscript{228} 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 “within a few short years we have fundamentally transformed our communications environment, turning our digital lives inside out.”\textsuperscript{229}

\textsuperscript{225} \textit{SCISA}, s 2. In \textit{Our Security, Our Rights: National Security Green Paper, 2016 [Green Paper]}, a “background document” meant to “prompt discussion and debate about Canada’s national security framework,” (at 1), the federal government justifies this concept on the basis that it “covers a broad range of national security-related activities” and is thus “intended to provide flexibility to accommodate new forms of threats that may arise.” Online: <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx>.

\textsuperscript{226} \textit{Criminal Code}, s 83.221(1).


One of the casualties of this assault on privacy has been freedom of expression. As documented in chapter one, there is a necessary connection between these rights, a speech-privacy continuum or matrix in which privacy, especially in relation to anonymity, promotes truly free, unrestrained speech and thought. With the introduction of SCISA and other state-sponsored anti-privacy initiatives, therefore, the impact is wider ranging than an attack on privacy as understood in the narrow sense of control over one’s personal information. In addition to this type of injury, protected by s. 8 (and, in certain scenarios, s. 7) of the Charter, one could as a function of government surveillance also suffer a rights restriction of the sort governed by s. 2(b). While the use of s. 2(b) to beat back privacy invasions has received little attention in the scholarship and case law on point, this possibility is being test driven in a 2015 application commenced in Ontario Superior Court by the CCLA and CJFE and a pair of 2014 cases brought in Federal Court by the BCCLA. These cases (and a prior effort by the CCLA to impugn 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 s. 2(b).

In what follows I will trace this use of s. 2(b) as a tonic to privacy breaches stemming from state surveillance practices, within and beyond the limits of Bill C-51. Just as the privacy right has been read into ss. 8 and (in a more circumspect manner) 7 of the Charter, I will argue that s. 2(b) is also triggered in some cases, especially in the online context, by invasive government interception, use and sharing of personal information. I first examine the privacy right, both as it has been enshrined in international law and as it has been read into, and excluded from, s. 2(b) and other Charter provisions. Next, I turn my attention to s. 2(b) itself, in the course of which I examine the continuity of speech and privacy, the chilling effects of surveillance and the impact
of technology on freedom of thought. This chapter concludes with an overview of the CCLA/CJFE and BCCLA litigation noted above, past and present, so as to track this privacy-focused approach to freedom of speech and thought in real time. I also in this final section review the advantages of s. 2(b) over s. 8 as a foil to state spying and possible practical evidentiary issues to remain alert to in the litigation context. Expanding the parameters of s. 2(b) thus, I argue, only enhances the menu of possible constitutional replies to privacy invasion, thereby helping to promote the transparency and oversight currently in short supply in our own surveillance society.

2 Privacy
2.1 The parameters of privacy

One of the most significant challenges in writing about privacy is the lack of consensus as to what this term actually signifies, conceptually and in practice, in any given context. In the most general sense, this evasive concept can be understood as an attempt to protect private information from the gaze of others but, upon further scrutiny and reflection, even this broad definition begins to quickly unravel. Most critically, perhaps, the very distinction between public and private realms has itself been rendered more complex of late with the advent of social media and other web platforms which allow, and in some sense require, us to live our private experiences in public. Also, as reviewed in this chapter, the troublesome issue of consent as it relates to such platforms and the harvesting and sharing of our personal information may vitiate any claim to a protected privacy zone. While it is true that certain differences exist between the freedom of expression right as set forth at s. 2(b) versus other national and international texts, such discrepancies do not take away from the collective understanding (if not promotion) of this guarantee across borders. Privacy, on the other hand, is a different beast entirely, and one is
confronted when attempting to speak about this slippery, multivalent topic with the task of imposing some measure of order on a plurality of moving parts.

This lack of conceptual clarity is routinely underlined by scholars, and constitutes a meeting point for many amidst the swirl of competing theoretical perspectives. Indeed, perhaps the one thing that many if not most seem content to agree on (other than the need to remain alive to the dangers of surveillance) is that, as Richards comments, “privacy can mean many things” and that “we often use [this word] without being clear about what we mean or why it matters.”230 He states: “scholars of privacy across disciplines have struggled to define the term, groping around with definitions that were too narrow or too broad, or giving up hope of defining it altogether,”231 a sentiment shared across the academic community. As Leslie A. Jacobs details, “there is no consensus on what we mean by ‘privacy rights,’”232 a reality described by Daniel J. Solove in paradoxical terms: “privacy seems to be about everything, and therefore it appears to be nothing.”233 For Solove, who has himself through his “taxonomy” sought to bring clarity and structure to this idea,234 privacy remains a “concept in disarray. Nobody can articulate what it means...Philosophers, legal theorists, and jurists have frequently lamented the great difficulty in reaching a satisfying conception of [it].”235 Perhaps Mark Tunick’s straightforward assessment

230 Supra note 11 at 103, 112. Richards continues: “one of the most difficult (and frustrating) things about privacy is that it has a bewildering variety of meanings. Sometimes it seems as if privacy can mean almost anything” (at 8).
231 Ibid at 8.
234 In Understanding Privacy (Cambridge, Ma: Harvard University Press, 2008) Solove creates a “taxonomy of privacy” comprising of four categories and sixteen subcategories designed to clarify the purpose and limits of privacy (at 101, 106-170).
235 Ibid at 1.
is the most realistic: “if one were to attempt to identify the essence of privacy – features common to all the different situations in which we would say that privacy is at stake – one might run into trouble.”

This lack of definitional clarity has not been lost on the Supreme Court of Canada, which has on a number of occasions taken notice of this particular difficulty. As early as Hunter v. Southam, a watershed case marking the start of “Canada’s constitutional discourse regarding privacy,” the court was forced to wrestle with the meaning of “unreasonable” in s. 8 and the legal limits of search and seizure. Dickson C.J.C., surveying this uncharted territory, anticipates future complications in defining privacy when he asserts: “it is clear that the meaning of ‘unreasonable’ cannot be determined by recourse to a dictionary, nor for that matter, by reference to the rules of statutory construction.” Future decisions of the court, focused more squarely on privacy per se rather than this part of the s. 8 apparatus, also stress the challenges of defining this idea. Thus in Dagg v. Canada (Minister of Finance), a case decided the following decade concerning access to information, Cory J. relates that “privacy is a broad and somewhat evanescent concept.” In 2004 Binnie J., in R. v. Tessling, concludes that “privacy is a protean concept,” a position re-stated in 2010 by Deschamps J. in R. v. Gomboc when she allows that

---


239 Supra note 237 at 155.

240 Supra note 173 at para 67.

241 Supra note 173 at para 25.
“privacy is a varied and wide-ranging concept.”
Most recently, in *R. v. Spencer*, Cromwell J. advises: “Scholars have noted the theoretical disarray of the subject and the lack of consensus apparent about its nature and limits.”

Just as the broader concept of privacy poses challenges for scholarship and adjudication, so too do the more narrow subsets of territorial, personal and informational privacy adopted by the Supreme Court of Canada create problems for critics and courts. Particularly in connection with the third category (notions of territorial and bodily integrity are more straightforward, relatively speaking, given perhaps their greater longevity and cultural resonance), which remains central to privacy law and analysis, the same difficulty arises: what kind of personal data does this informational basket contain and how are such contents affected by a multiplicity of factors? While the Supreme Court of Canada has established a baseline “biographical core” litmus test to assist with these questions, it remains unclear if this provides sufficient direction on the threshold “reasonable expectation of privacy” analysis at the centre of s. 8. Craig Forcese and Kent Roach, for their part, do not appear to think so, speaking of a “jurisprudence as clear as mud” and offering that the exact meaning of informational privacy and the “biographical core” are “in the eye of the beholder.” And, just to muddy the waters even further, there is now a tendency when speaking of such issues, especially in light of the contemporary surveillance scare, to conflate informational privacy with privacy writ large and notions of corporeal and

---

243 *Supra* note 1 at para 35.
244 *Ibid*.
245 *Ibid* at para 27.
246 *Supra* note 7 at 122.
terриториal integrity. As Janice Richardson recounts: “today, the term 'privacy' often denotes informational privacy.”

While unhelpful for obvious reasons, it can be argued that this definitional quagmire does have an upside, especially in Canada and other jurisdictions which have not formally adopted a standalone privacy right (as opposed to protecting privacy through the back door by means of s. 8 or some cognate mechanism). This conceptual fluidity, in addition to posing problems, might equally prove beneficial in situations where one needs the privacy construct to serve a number of different functions. In the Canadian context, as is canvassed more fully below, in the absence of a Charter privacy guarantee, a flexible approach has allowed for the identification of privacy themes across distinct issues and scenarios. Thus, for example, this concept is as much at home in constitutional 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 canvass onto which to project existing and future possibilities for continued judicial expansions of privacy protections north of the forty-ninth parallel. Obviously, this is directly relevant to the application of s. 2(b) in this context, and affords champions of this vision of free speech a sturdier basis for doing so than might otherwise be available were the contours of the Charter privacy landscape more firmly set in stone.

This breadth of meaning has been hit upon by critics who, in addition to pointing out the difficulty of defining privacy, characterize it as encompassing multiple concepts simultaneously. This point is flagged by Alysia Davies, who chronicles that “many commentators…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.”

Richards, too, says as much, reporting that “in recent years, many scholars have settled on an understanding of privacy as an umbrella term that encompasses a variety of related meanings.” Jacobs also tracks this trend to emphasize such polyvalence: “the right to privacy can be understood as a cluster concept, by which we mean it involves a cluster of different ideas that can be arranged in a variety of ways.” In the end, this may prove to be the least problematic interpretative approach, since any effort to nail privacy down conclusively will, not unlike the game of whack-a-mole, only generate additional questions and issues. So while the alphabet soup of competing interpretations might at some level be viewed as “theoretical disarray,” it does at the same time have much to recommend it, not least of which is its potential for unlocking constitutional possibility, in Canada or elsewhere. As Lillian BeVier phrases it: "Privacy is a chameleon-like word, used...connotatively to generate goodwill on behalf of whatever interest is being asserted in its name.”

### 2.2 Privacy rights abroad and (almost) in Canada

The right to privacy has been recognized in a variety of national and international legal texts around the world. At the international level, it is guaranteed under a number of agreements,

---

249 *Supra* note 11 at 9.
250 *Supra* note 232 at 5-6.
including article 12 of the 1948 *Universal Declaration of Human Rights* ("UDHR"), which protects individuals against “arbitrary interference with…privacy, family, home or correspondence.” Article 17 of the 1966 *ICCPR* sets out this principle in largely the same terms, establishing in part that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.” And, building on these United Nations documents, regional texts like the *European Convention on Human Rights* ("ECHR") and the *American Convention on Human Rights* also protect privacy. Domestically, some jurisdictions have extended such protection by introducing a privacy component directly into their national constitutions. Title II, Chapter I, Article 5 of the Brazilian constitution provides that “the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured.” In South Africa, chapter 2 of the constitution (also known as the Bill of Rights) instructs: “Everyone has the right to privacy,” a right protecting against the search of home and property, the seizure of possessions and the infringement of personal communications.

---

253 *UDHR*, art 12.
254 *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171 art 17 [*ICCPR*].
256 *American Convention on Human Rights*, 22 November 1969, 1144 UNTS 143 art 11 [*ACHR*].
257 *Constitution of Brazil*, 5 October 1988, title II, c I, art 5.
258 *Constitution of the Republic of South Africa*, 1996, No 108 of 1996, c 2. Various national constitutions include a formal privacy component. For a useful means of identifying and comparing such instruments see Constitute, a project developed by the authors of the Comparative Constitutions Project at the University of Texas at Austin, online: <https://www.constituteproject.org>.
In Canada there is no overarching right to privacy, separate and apart from the privacy protections which have been read into specific provisions of the Charter. In the absence of a singular law of this kind, we must content ourselves with a patchwork of national and provincial legislation which, collectively, goes some distance toward plugging this constitutional hole. With respect to personal information held by the federal government, one must rely on the Privacy Act and, in Ontario, individuals seeking to protect and access this information in the custody of provincial or municipal actors may turn to the Freedom of Information and Protection of Privacy Act or the Municipal Freedom of Information and Protection of Privacy Act respectively. For those in need of assistance in relation to personal data in the possession of private sector entities, there is the Personal Information Protection and Electronic Documents Act or, where available, equivalent sub-national substitutes. While these tools can prove helpful, however, they lack the constitutional imprimatur which would prevent them from being trumped by other statutes. To take but one example, were the Privacy Act accorded such status, its network of exemptions at s. 8(2) (and, in particular, the reference to “any Act of Parliament or any regulation made thereunder” at s. 8(2)(b)) would be unable to impair its objective of protecting against threats like SCISA.

259 Privacy Act, RSC, 1985, c P-21.
262 Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
263 Forcese and Roach remark in connection with the Privacy Act that it “says, in essence, ‘no sharing, but…’ And the ‘but’ or justifications for sharing are exceptions that practically gut the rule” (supra note 7 at 162). For the federal government perspective on such Privacy Act exceptions see the Green Paper, supra note 225 at 26-27.
Things almost turned out differently. When one reviews the committee and Parliamentary debates leading up to the coming into force of the Charter in 1982, one realizes that, in fact, Canada came very close to adopting a stand-alone constitutional right to privacy of the sort found in international and domestic instruments surveyed above. Although it may prove difficult to appreciate more than three decades after the fact, Part I of the Constitution Act, 1982 was not pre-ordained to look the way it does today. Like any other piece of legislation, it was the product of much negotiation and argument between denizens of the Hill. Much of this intellectual heavy lifting was overseen by the Special Joint Committee of the Senate and of the House of Commons on the Constitution of Canada (“Committee”), led by joint chairmen Senator Harry Hays and Minister of Parliament Serge Joyal.\footnote{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 (20 January 1981) at title page [Minutes of Proceedings and Evidence].} Tasked with the awesome responsibility of shaping the constitutional future of the country, the Committee spent hours, days and weeks parsing the Trudeau government’s proposed Charter. In doing so they endeavoured, amongst Committee members and the witnesses invited to speak to specific topics, to refine the message and mechanics of this text. It is during this period of frenzied activity and political horse-trading that Canada nearly adopted a separate privacy right of its own.

On January 20, 1981, Jake Epp, a member of the Committee, urged on behalf of the Progressive Conservative party that “Clause 2” of the draft Charter dealing with “fundamental freedoms” be expanded to include a fifth section. This addition, s. 2(e), guaranteed “freedom from unreasonable interference with privacy, family, home, correspondence, and enjoyment of...
property.”265 As related by Epp, this privacy right, which mirrored the relevant provisions of the UDHR and the ICCPR, was meant to ensure that “all Canadians who have come to our country in search of freedom and security, will be protected from the arbitrary encroachment of any government on many aspects of their individual lives.”266 Two days later, on January 22, David Crombie, a fellow Progressive Conservative, echoed Epp’s presentation on the 2(e) privacy right, tracing its similarities with the United Nations texts and pointing out for Committee members its commonalities with the “specific constitutions of very specific countries.”267 Further support for this amendment came from across the political aisle, as Sven Robinson, on behalf of the New Democrats, pressed that it “should be reflected in the proposed Charter of Rights.”268 Although regularly unable to agree on much, the Canadian left and right nonetheless found common ground, at this juncture in early 1981, in their effort to secure constitutional protection for the private sphere.

Not all members of the Committee, however, were equally enthused by the prospect of the s. 2(e) amendment. In particular, Jean Lapierre, part of the Trudeau Liberal team, argued that the “wide array of protections”269 afforded by s. 8 would suffice for privacy-related concerns, especially since (anticipating the present day commentary cited above) privacy is itself a “fairly vague concept.”270 More particularly, what gave Lapierre pause was that, “given the present notions of the law, it is a concept too vague and ill defined” and “we could wonder what kind of

265 Ibid at 97.
266 Ibid.
267 Ibid No 43 (January 22, 1981) at 57.
268 Ibid at 61.
269 Ibid at 58.
270 Ibid.
interpretation the courts would give to that concept.”

Crombie, in response, noted that many privacy problems fell beyond “search and seizure” and thus required a constitutional tool in addition to s. 8. He added: “It may be vague to Mr. Lapierre but I think there are a number of people who would like to have a freedom that says they are protected particularly from government in relation to their own privacy.”

Such remarks do not in the end appear to have swayed the Committee, and the amendment to Clause 2 was defeated on January 22 by four votes, as recounted in the Committee records: “it was negatived on the following show of hands: YEAS: 10; NAYS: 14.” But for a handful of votes, in other words, the Charter might well have contained, alongside the s. 2(b) freedom of expression guarantee, a right to privacy.

In the days and months following this defeat, members of both the Progressive Conservatives and the New Democrats attacked this result in the House of Commons and continued to underscore the need for privacy protection. Exactly one week after the 10-14 vote, on January 29, Robinson spoke at length on the topic, channelling Orwell in invoking “Big Brother” and admonishing that “as we approach the 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.”

Perrin Beatty, a Progressive Conservative, also took issue with the January 22 result, stating 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

271 Ibid.
272 Ibid at 60.
273 Ibid.
274 Ibid at 7.
that is the right to privacy.”\textsuperscript{276} The next month, another conservative politician, Walter Baker, again highlighted (in the course of a debate on Bill C-238, entailing communication interception-related amendments to the \textit{Criminal Code}\textsuperscript{277}) that “one of the most fundamentally important rights of a citizen in a free society is that of privacy” and that there was a need for protections against “inappropriate snooping by police and authorities, however well intentioned.”\textsuperscript{278} As he put it: “the electronic age is upon us and, as technology grows, the potential for that kind of interference grows as well.”\textsuperscript{279}

### 2.3 Reading privacy into the \textit{Charter}

In the years following the “negatived” vote of January 22, 1981, the concept of privacy, while not formally granted a provision of its own, either under the s. 2 umbrella or elsewhere in the \textit{Charter}, has made inroads toward constitutional recognition. While Canadians are, technically speaking, no further ahead than they were in the days of the Committee toward achieving such a stand-alone guarantee, our courts have in the intervening period recognized the singular importance of privacy in a free and democratic society. Recalling the arguments of Crombie, Robinson and others before the Committee and in the House of Commons, judges have read s. 8 through the privacy lens (as per Lapierre’s approach in 1981) and have, more and more, come to identify this interest in s. 7 as well. Justice La Forest, a well-known privacy booster, asserts in \textit{R. v. Dyment} that it is “worthy of constitutional protection” since it is “at the heart of liberty in a modern state…Grounded in man’s physical and moral autonomy, privacy is essential for the

\begin{itemize}
\item \textsuperscript{276} \textit{Ibid} at 6704.
\item \textsuperscript{277} \textit{Ibid} No 7 (February 20) at 7538.
\item \textsuperscript{278} \textit{Ibid} at 7539.
\item \textsuperscript{279} \textit{Ibid}.
\end{itemize}
well-being of the individual.” Writing nearly a decade later, this time in dissent, he elaborates this theme somewhat, commenting in Dagg that the “protection of privacy is a fundamental value in modern, democratic states” because, as an expression of one’s “unique personality or personhood,” it is “grounded on physical and moral autonomy – the freedom to engage in one’s own thoughts, actions and decisions.”

Due in no small part to the work of La Forest J. in Dagg, Dyment and other cases, the Supreme Court of Canada has bestowed upon privacy legislation a quasi-constitutional status, a step up from the January 1981 Committee result. As explained by Abella and Cromwell JJ. 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.” While much of the case law on point focuses on the “special nature” of the Privacy Act, one assumes that this “quasi-constitutional” mantle is also applicable to other (existing or future) federal, provincial and territorial laws of this sort. This approach to privacy, which for Davies signals an “overlooked Charter right,” suggests for Jacobs “hermeneutic rights to privacy” which, though they “may not receive explicit recognition in the Constitution Act, 1982, [are] closely tied to existing constitutional rights and values.”

---

280 Supra note 173 at para 17.
281 Supra note 173 at para 65.
282 Supra note 77 at para 19.
284 Supra note 248 at 261.
285 Supra note 232 at 23.
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.”

The original locus for this “implicit constitutional right” was s. 8 of the Charter, a jurisprudential move first tested in Hunter v. Southam where, as stated 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.” This use of s. 8 as a vessel for certain privacy-related issues cannot have come as much of a surprise in 1984, when Hunter v. Southam was rendered, given its explicit focus on unreasonable search and seizure and the necessary connection of such violations to the private sphere. Indeed, at least one member of the Committee: Lapierre, seemed wholly comfortable with the hitching of s. 8 to the privacy wagon, and subsequent decisions of the Supreme Court of Canada and other courts have tended to closely follow suit. Many if not most of the foundational “privacy” judgments are rooted in this provision, up to and including Spencer, which propelled the case law into the twenty-first century through its attention to online activity and the role of internet service providers in disclosing personal subscriber information. If one were forced to identify a part of the Charter which most transparently filled the privacy gap, s. 8 would clearly be it. It is important to remember, however, that

---

287 Supra note 173 para 19.  
288 Supra note 1 at para 5.
although this *Charter* provision may be the most usual suspect in this regard, it has not cornered the market by any means.

Perhaps as a function of the “ill-defined” nature of privacy, which concerned Lapierre in January 1981 and may have doomed the 2(e) proposal advanced by Epp, Crombie and their parliamentary colleagues, the Supreme Court of Canada has, beyond s. 8, read a privacy component into s. 7. In some sense fulfilling Lapierre’s worry that this “fairly vague concept” could open up the “kind of interpretation the courts would give to [it]” the court has expanded the purview of our implicit, unofficial privacy right along these lines. The evolution of s. 7 in this regard is of particular interest since, unlike s. 8, whose connections to this right are plainly obvious, the “life, liberty and security of the person” angle may not at first blush be readily apparent. With respect to s. 7, any such link is less straightforward (since, for one thing, its text does not invoke the public-private divide to the same extent as “unreasonable search and seizure”) and there is more conceptual legwork, it can be argued, to get from A to B. It may have been for this reason that Dickson C.J.C., in his 1988 ruling in *R. v. Morgentaler*, declines to interpret s. 7 within a privacy framework. Rejecting the argument that this part of the *Charter* is “wide-ranging” and includes “a right to privacy,” he concludes that “it is neither necessary nor wise in this appeal to explore the broadest implications of s. 7.” As he specifies, “I do not

---

290 Ibid.
291 *R v Morgentaler*, [1988] 1 SCR 30 at paras 10-11, 44 DLR (4th) 385 [*Morgentaler*]. See also *R v Rowbotham*, 11 CRR 302, 42 CR (3d) 164, a decision of the Ontario High Court of Justice in which Ewaschuk J., referencing the Committee’s rejection of the 2(e) proposal, pronounces: “Mr. Horkins has submitted that the right to security of the person granted by s. 7 of the Charter creates a right to privacy or, in the alternative, various zones of privacy. I also reject this argument. While I concede that the right to privacy may be a value underlying various Charter
think that it would be appropriate to attempt an all-encompassing explication of so important a provision…so early in the history of Charter interpretation.”

Wilson J., writing in this same judgment, takes a different view, holding that the s. 7 interpretation is central to the litigation and that, accordingly, “the Court must tackle the primary issue first.” Proceeding on this basis to start her analysis with this “central issue,” Wilson J. thereby takes up the question deflected by the Chief Justice, opining 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.” This finding has since been affirmed on a number of occasions, thus allowing s. 7 to join s. 8 as one of the few Charter rights identified by the Supreme Court of Canada as protecting privacy interests. As stated by La Forest J. in R.B. v. Children’s Aid Society of Metropolitan Toronto in connection with Wilson J.’s statement in Morgentaler: “While I was in dissent in that case, I agree with this statement, and, indeed, I later observed in R. v. Beare…that I was sympathetic to the view that s. 7 of the Charter included a right to privacy.” L’Heureux-Dubé J., in her R. v. O’Connor decision penned the same year, further brings this point home: “This Court has on many occasions recognized the great value of privacy in our society” and

---

292 Morgentaler, ibid at para 11.
293 Ibid at para 221.
294 Ibid.
295 Ibid at para 230.
296 Supra note 201 at para 81.
“has expressed sympathy for the proposition that s. 7 of the Charter includes a right to privacy.”

In reviewing the manner in which privacy has been read into s. 8 and, in particular, s. 7, one gains insight into the fact that this is a somewhat elastic process and that, accordingly, this interpretative method is not limited to these two rights. Stated differently, given the absence of any dedicated privacy right and the looseness of this concept, there is no reason why this hunt for privacy shelter should end with these two Charter provisions. Daphne Gilbert has taken this position, maintaining that “this positioning of privacy in the Legal Rights section alone neglects privacy’s relevance to other Charter guarantees.”

Making the pitch that privacy should also be located in s. 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” by ss. 7 and 8. To stop here, she proposes, creates an “impoverished interpretation of what privacy could offer to human rights protections in Canada” and an “incomplete and inadequate vision of a constitutional privacy interest.” For her, “finding a home” for privacy beyond the parameters of ss. 7 and 8 “opens new possibilities for expanding

---

297 Supra note 201 at para 110. 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 para 58, 55 DLR (4th) 481; Edmonton Journal, supra note 18 at para 90; Dagg, supra note 173 at para 66; AM v Ryan, [1997] 1 SCR 157 at para 79, 143 DLR (4th) 1; Godbout v Longueuil (City), [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.


299 Ibid at 145.

300 Ibid at 139.

301 Ibid at 144. Mayeda 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” (supra note 102 at 60, 83-84).
its constitutional protection and its utility as a tool in advancing other Charter rights.” Turning now to examine freedom of expression, I take up this argument on behalf of s. 2(b), outlining how it too has recently been endorsed as an effective riposte to invasions of our online activity.

3 Freedom of expression
3.1 The free speech-privacy connection

As outlined in chapter one, there exists a necessary connection between freedom of expression and privacy which, I suggest, makes s. 2(b) ripe for inclusion in that collection of Charter rights isolated, as it were, as privacy-friendly. Just as ss. 7 or 8 (or 15, as per Gilbert) could be approached in this way, it makes sense that this same treatment would be applied to s. 2(b), 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, Cromwell J.’s hotly debated ruling, in addition to confirming that individuals possess 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 canvassed in several judgments focused on cyberspace defamation, *Spencer* was the first substantive foray by the Supreme Court of Canada into such issues, especially vis-à-vis internet expression. Citing the work A. F. Westin, Cromwell J. reminds his reader that “anonymity permits individuals to act in public places but to preserve freedom from identification and

---

302 *Ibid* at 139.
surveillance,” a reality of “particular…importan[ce] in the context of Internet usage.”

Cromwell J. singles out, as stated above, that “form of anonymity” critical to the author “who wants to present ideas publicly but does not want to be identified,” one of the “defining characteristics of some types of Internet communication.”

Although Spencer may be the most significant Supreme Court of Canada decision to date dealing with the intersection of expression and privacy, is it not the first time that this court has taken notice of the complementarity of these two fundamental interests. My review of the case law in chapter one establishes that it has on a number of earlier occasions signalled the possibility of such a mash-up of constitutional principles. To recap: in Canada (Human Rights Commission) v. Taylor, Dickson C.J.C., contrasting the extent and nature of hate speech protection in s. 319(2) of the Criminal Code (which does not apply to private communications) with that in s. 13(1) of the Canadian Human Rights Act (which does), opines in acknowledging this legislative difference

---

303 Supra note 1 at para 43. From the federal government perspective, Spencer is problematic in limiting access to certain types of information in a law enforcement context. As explained in the Green Paper, supra note 225 at 63: “Since the Spencer decision, police and national security agencies have had difficulty obtaining BSI [basic subscriber information] in a timely and efficient manner. This has limited their ability to carry out their mandates, including law enforcement’s investigation of crimes.” The Privacy Commissioner of Canada, for his part, takes a different view in endorsing the findings in Spencer (Time to Modernize, supra note 227 at 23-24), and Forcese and Roach have along similar lines questioned the value of the Green Paper’s second guessing of Spencer. See Craig Forcese & Kent Roach, “Righting Security: A Contextual and Critical Analysis and Response to Canada’s 2016 National Security Green Paper” (2016) at 32-33, online: Social Science Research Network <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849261>. For a discussion of the types of security concerns outlined in the Green Paper, pre-Spencer, see Robert W Hubbard, Peter DeFreitas & Susan Magotiaux, “The Internet – Expectations of Privacy in a New Context” (2001) 45 Crim LQ at 170.

304 Ibid at para 45.

305 Ibid.
that the “connection between s. 2(b) and privacy is thus not to be rashly dismissed.” The following decade, the new Chief Justice, McLachlin C.J.C., again highlights this link in *R. v. Sharpe* when she defines privacy not merely in terms of ss. 7 and 8 but also in relation to s. 2(b). She clarifies: “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.”

Taken together, these three decisions, rendered in 1990, 2001 and 2014, reflect the court’s ongoing recognition of this pairing of rights over many years.

Further, beyond the Supreme Court of Canada, other courts have taken notice of the various ways in which privacy and speech interact. In the defamation context, as I have explained, leading cases like *Warman v. Wilkins-Fournier* and *King v. Power* rendered by the Ontario Divisional Court and the Newfoundland and Labrador Superior Court respectively, explore the impact of anonymity on reputation and online expression. The Alberta Court of Queen’s Bench, in *Harper v. Canada (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. remarks, citing *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

---

306 *Supra* note 187 at para 193.
307 *Supra* note 190 at para 26.
308 *Supra* note 181.
309 *Supra* note 183.
strengthen a claim under s. 2(b) of the Charter.”\textsuperscript{310} In the lower court Sharpe decision, similarly, Shaw J. of the British Columbia Supreme Court shares (again relying on Taylor) that the “case law on freedom of expression reflects the Charter's concern for the right of privacy.”\textsuperscript{311} Even in the pre-Charter period, courts were alert to this feature of free speech. Berger J., writing in \textit{R. v. Bengert (No. 8)} in 1979, strikes a decidedly modern note: “With the advance of technology, the possibilities for the infringement of privacy have proliferated…the right of privacy…is essential to freedom of thought and freedom of speech.”\textsuperscript{312}

Whatever the specific focus of these decisions, they collectively signpost an emerging view, most recently articulated by Cromwell J. in \textit{Spencer}, of the working relationship between expression and privacy. As outlined previously, these interests have frequently been characterized, by commentators and courts, as being opposed in interest, a long-championed construct of speech (and freedom of the press in particular) versus the private sphere featured in multiple Supreme Court of Canada judgments and the famous Warren and Brandeis article \textit{The Right to Privacy}.\textsuperscript{313} That said, decisions like the ones just reviewed present the other side of the coin: the possibility, and in certain cases necessity, of harnessing privacy as a vehicle for expressive freedom. This body of law, touching on different topics across criminal and civil proceedings, tracks the emergence of an expansion of s. 2(b) along similar lines, I would suggest, as that evidenced with respect to ss. 7 and 8 of the Charter. Just as courts have read a privacy component into these constitutional provisions (a more gradual process in terms of s. 7), such

\textsuperscript{311} R v Sharpe, 69 DLR (4th) 536, [1999] BCJ No 54 (QL) at para 44.
\textsuperscript{312} R v Bengert, Robertson (No. 8), 15 CR (3d) 37, [1979] BCJ No 1709 (SC) (QL) at para 5.
\textsuperscript{313} Supra note 53.
jurisprudence telegraphs that “instead of being conflicting values, privacy and speech can instead be mutually supportive.”\textsuperscript{314} It would seem reasonable to suggest, therefore, that s. 2(b) has also come to provide a “new home” for this right, as Gilbert might put it,\textsuperscript{315} given the ways in which this connection has been pinpointed by the Supreme Court of Canada and lower courts across Canada.

Reading s. 2(b) as encompassing protection against privacy violations also makes sense, beyond this body of supporting case law, in terms of broader principles of statutory interpretation regularly applied to this Charter provision. As is routinely stated, s. 2(b) is intended to be understood and applied in a permissive, expansive manner. This mantra finds early expression in Irwin Toy Ltd. v. Québec (Attorney General), where the Supreme Court of Canada establishes that the “content of expression can be conveyed through an infinite variety of forms of expression” and accordingly calls for a “broad, inclusive approach to the protected sphere of free expression.”\textsuperscript{316} More recently, in Baier v. Alberta, LeBel J. repeats this position in summarizing that “the Court has traditionally defined freedom of expression in broad terms.”\textsuperscript{317} Quoting an earlier Supreme Court of Canada decision, he continues 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.”\textsuperscript{318} McLachlin C.J.C., in Sharpe, provides context for such breadth by highlighting the singular function played by s. 2(b), depicted by her

\textsuperscript{314} Richards, supra note 11 at 95.
\textsuperscript{315} Supra note 298 at 139.
\textsuperscript{316} Irwin Toy Ltd. v Québec (Attorney General), [1989] 1 SCR 927 at paras 42-43, 58 DLR (4th) 577.
\textsuperscript{317} Baier v Alberta, 2007 SCC 31 at para 90, [2007] 2 SCR 673.
\textsuperscript{318} Ibid at para 91. See also Hogg, supra note 32 at 43:9-10; Sharpe and Roach, supra note 32 at 157.
as being “among the most fundamental rights possessed by Canadians,” a guarantee which “makes possible our liberty, our creativity and our democracy.”

Following in the footsteps of the “life, liberty and security of the person” make-over, s. 2(b) would appear to be taking its place alongside ss. 7 and 8 as a constitutional provision to be marshalled in the face of state-sponsored privacy violations. Evincing the “living tree” nature of the Canadian constitution, as it was dubbed by Lord Sankey in 1930, this ongoing evolution of s. 2(b) might in some sense be seen as a vindication for those Parliamentarians who fell short in their 1981 attempt to secure the s. 2(e) right of “freedom from unreasonable interference with privacy.” As the spectre of government surveillance grows and professional critics and regular citizens become more alert to this reality of our web-soaked universe, it makes sense that this dimension of s. 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 certain circumstances and, just like ss. 7 and 8, would be pleaded accordingly. And while it is certain that any such use of s. 2(b) would almost certainly result in cross-over with other Charter provisions (most likely s. 8), challenging state action on multiple, at times overlapping grounds is a common litigation strategy. In the end, there is little downside in adding free speech to the Canadian constitutional privacy mix, especially given the growing threat to our online information security.

---

319 Supra note 190 at para 21.
3.2 Grave new world of online surveillance

As noted in chapter one, 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 printing technology in fifteenth century Europe. Canadian courts have acknowledged 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.”\(^{321}\) Abella J., speaking for the majority of the Supreme Court of Canada in *Crookes v. Newton*, which examines the link between defamation and hyperlinks, instructs that the “Internet’s capacity to disseminate information has been described by this Court as ‘one of the great innovations of the information age.’”\(^{322}\) This comes as no surprise, certainly, as we take for granted (at least in wealthy first world communities) that the ubiquitous online universe has shaped many if not most aspects of our lives. As expressed by Nicola Dalla Guarda, “in this day and age it has become cliché to say that the internet has come to permeate every facet of our lives.”\(^{323}\) Indeed, gone are the days when a connection to cyberspace was seen by many as an optional luxury, to the extent that there is now a movement afoot to characterize such access as a human right.\(^{324}\) As Paul Bernal is quick to point 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.”\(^{325}\)

---


\(^{324}\) See, for instance, Karanicolas, *supra* note 129.

\(^{325}\) *Supra* note 66 at 2.
As with every plus, however, there is a downside to the increasing global access to the internet and our growing dependence on this technology for an expanding set of diurnal tasks, no matter how mundane. 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 which has greatly enhanced the threat of surveillance creep. This paradox: the simultaneous facilitating and shutting down of freedom, is a fact of contemporary life and looms large in academic and other discussions of Bill C-51 and similar state initiatives. Davies is downbeat on point, bemoaning 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.”

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 liberating technologies…have instead ushered in an era of surveillance” 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.”

---

326 Supra note 248 at 265.
328 Supra note 11 at 2.
One of the first casualties of this grave new world, then, is privacy, as government actors (at times with the intentional or unwitting help of corporations) follow the data trail in pursuit of villains and other national security threats. Although it goes without saying, particularly given the present epidemic of terrorist-related violence, 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 deployed 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.” In his re-telling of the Snowden saga, likewise, Glenn Greenwald isolates this central feature of post-9/11 thinking, arguing that the “opportunity those in power have to characterize political opponents as ‘national security threats’ or even ‘terrorists’

329 Critics have catalogued the ways in which corporations are complicit in undermining online privacy and free speech. As Austin proposes, if “we want to revive privacy from its current death throes, attending to the activities of state authorities is not enough. We need to understand the business model of surveillance and the role of law in enabling both it and the corporate–state nexus” (supra note 218 at 132). See also Deibert, supra note 229 at 197-198; Richards, supra note 11 at 174; Jacobs, supra note 232 at 2-3; Bernal, supra note 66 at 55; Price supra note 327 at 34; Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA and the Surveillance State (Hamish Hamilton: London, 2014) at 170.

330 Such overreaching is not, of course, restricted to Bill C-51 and the contemporary national security scene, and has been referenced by courts in various earlier judgments. To take but one example, see La Forest J.’s s. 8 discussion of electronic surveillance and risk analysis in R v Duarte, [1990] 1 SCR 30, 65 DLR (4th) 240 at paras 10-33.

331 Supra note 117 at 52. John Stuart Mill, in his 1859 tract On Liberty, specifies that this marriage of security and surveillance is a long-standing political strategy: “The ancient commonwealths thought themselves entitled to practise, and the ancient philosophers countenanced, the regulation of every part of private conduct by public authority, on the ground that the State had a deep interest in the whole bodily and mental discipline of every one of its citizens…in constant peril of being subverted by foreign attack or internal commotion” (supra note 118 at 30). Lyon also speaks to the longevity of surveillance tactics: “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 220 at 22).
has repeatedly proven irresistible.”

The gist of this view is seconded 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.’” On the basis of such “vague and unspecified notions of ‘national security,’” privacy and freedom of expression are now under attack, both in Canada and around the planet.

In 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 written, Jeremy Bentham’s idea of the Panopticon, a prototype of the Big Brother trope introduced over one hundred and fifty years later, is an apt metaphor for the chilling effects of such surveillance. A prison in which inmates are housed along the perimeter 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.” Not entirely unlike this eighteenth-century penal institution, certain components of Bill C-51 and similar instruments could be said to chill expression. Critically, the

---

332 Supra note 329 at 186.
333 Supra note 248 at 263.
334 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 23rd Sess, (17 April 2013) at para 58, online: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement>. Earlier in the report he comments: “Concerns about national security and criminal activity may justify the exceptional use of communications surveillance technologies. However, national laws regulating what would constitute the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or non-existent” (at para 3).
335 See, for instance, Richards, supra note 11 at 104; Greenwald, supra note 329 at 175.
337 Orwell, supra note 223 at 5.
338 Bentham, supra note 336 at 45.
point here is not that one must be aware that he or she is being monitored but, rather, that the mere reasonable apprehension of this monitoring could trigger a speech problem. This dynamic, that “even the perception of being surveilled can have a chilling effect,”\footnote{Jillian York, “The harms of surveillance to privacy, expression and association” in \textit{Global Information Society Watch 2014: Communications surveillance in the digital age} at 29, online: \url{http://giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf} \citep{GlobalInformationSocietyWatch}.} is a common theme in the literature, a leitmotif which recurs again and again in analyses of the impact of state snooping on online freedom.\footnote{See, for example, Richards, \textit{supra} note 11 at 104; Price, \textit{supra} note 327 at 29; Greenwald, \textit{supra} note 329 at 2-3; Cockfield, \textit{supra} note 117 at 52; 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, \textit{Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century} (The Hague: Asser Press, 2014) at 253. As William Kowalski plainly articulates the problem in a February 4, 2015 PEN Canada blog post: “And in case you’re wondering what privacy has to do with freedom of expression, it’s very simple: How can you be expected to express yourself freely if you’re worried about who might be listening.” Online: \url{https://pencanada.ca/blog/does-cse-know-too-much-about-us}.} Like Bentham’s prisoners, persons with some realistic sense that they are under scrutiny, and who as a result decide not to make this or that statement for fear of reprisal, might well be able to argue cogently that their liberties have been abridged.\footnote{See my analysis of the CCLA and BCCLA cases below regarding how this chilling effect has been characterized and attacked in \textit{Charter} challenges to Bill C-51 and similar Canadian legislation.}

In the wake of the Snowden leaks, much attention has focused on the U.S. government spying undertaken by the National Security Agency, although it continues to become apparent that Canada too has been quite 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\footnote{As detailed in a report prepared by Privacy International and Amnesty International: “The Five Eyes Alliance is a secretive, global surveillance arrangement of States comprised of the}} has been busy
sorting through a massive amount of intercepted online communications in a needle in a
haystack\textsuperscript{343} effort to detect potential security threats. Referencing a Canadian “spying initiative”
with the code name Levitation, Greenwald and Ryan Gallagher report that the “Canadian
government has launched its own globe-spanning Internet mass surveillance system.”\textsuperscript{344} Or, as
per 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.”\textsuperscript{345} And while Ottawa
might insist that any such program targets foreigners exclusively, the discovery, care of
Snowden, that CSE had tapped into an internet server at a “major Canadian airport” has led
experts to challenge this claim.\textsuperscript{346} Given this covert operation, and troubling federal powers like

\textsuperscript{343} Forcarse and Roach seize on this metaphor: “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...The SoCIS Act risks more of the disease of agencies drowning in data”
\textit{(supra note 7 at 166). 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 229, 183 at 186.}

\textsuperscript{344} Ryan Gallagher & Glenn Greenwald, “Canada casts global surveillance dragnet over file
downloads”, \textit{The Intercept} (18 January 2015), online:
\url{https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance}.

\textsuperscript{345} Amber Hildebrandt, Dave Seglins & Michael Pereira, “CSE tracks millions of downloads
daily: Snowden documents”, \textit{CBC News} (27 January 2015), online:
Security Establishment’s cyberwarfare toolbox revealed”, \textit{CBC News} (2 April 2015), online:
\url{www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolboxrevealed-1.3002978}.

\textsuperscript{346} Greg Weston, Glenn Greenwald & Ryan Gallagher, “CSEC used airport Wi-Fi to track
Canadian travellers: Edward Snowden documents”, \textit{CBC News} (30 January 2014), online:
the snooping authorized under the *CSIS Act*\(^{347}\) and SCISA’s information-sharing regime, there is every reason to think that our internet freedoms are in jeopardy, at home as well as abroad.

And this is where s. 2(b) comes into play. In such a scenario, which itself is anchored in a privacy violation, the chilling of expression flowing from this initial interference falls precisely within the ambit of a privacy-responsive free speech right. Although the injured party could in this case also attack this invasion of the private sphere on the basis of s. 8 (s. 7 is, I think, largely unhelpful here), it is s. 2(b) which is the clear choice for targeting this chilling effect. To the extent that victims are able to show that state surveillance impinges on their ability to “express their opinions or communicate with other persons for fear that they will face sanctions,”\(^{348}\) they could make use of this provision, either on its own or in conjunction with s. 8. Because “mass surveillance violates both the right to privacy and to freedom of expression,”\(^{349}\) it makes sense that s. 2(b) would feature in any challenge to such activity touching on expression, as well as or instead of search and seizure. In a sense, making use of s. 2(b) thus could be seen as tapping into the potential of s. 2(e), a constitutional project that died on the Committee floor in 1981 before ever seeing the light of day. It is noteworthy that Epp, Crombie and their fellow Progressive Conservatives chose “Clause 2,” which already housed free speech, for their proposed privacy

\(^{347}\) As explained below, such CSIS powers were unsuccessfully challenged by the CCLA in the 1990s.


right, as if confirming through the structure of the *Charter* itself the continuity of these two interests.

### 3.3 Freedom of thought

It is easy to forget, in exploring the privacy component of s. 2(b), that this constitutional provision concerns at least two distinct concepts: freedom of speech and freedom of thought. While certainly related, these twin concepts are substantively different, a fact which is overlooked in the Canadian context for a number of reasons. First, both are included within the same section of the *Charter*, which lists off “freedom of thought, belief, opinion and expression” in a single phrase as if bringing them all together without much if any distinction. But, when one reviews the staple international agreements, it becomes clear that the yoking of these rights is far from standard in these texts. In many of these instruments, thought and speech, while often addressed in neighbouring articles, are treated separately, usually along the lines of “freedom of thought, conscience and religion” versus expression, as is the case in the *UDHR* (articles 18 and 19), *ICCPR* (articles 18 and 19), and *ECHR* (articles 9 and 10). Here, the right to think for one’s self, an internal intellectual and existential 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 in the fact that the *Charter* incorporates freedom

---

350 *Supra* note 116.
351 *Supra* note 254.
352 *Supra* note 255. Note, however, that this is not always the case. The ACHR, for example, groups thinking and speaking together, addressing “freedom of conscience and religion” at article 12 and “freedom of thought and expression” at article 13 (*supra* note 256). Of course, it is not always easy to distinguish speech from thought. As McLachlin C.J.C. states in *Sharpe*: “The distinction between thought and expression can be unclear. We talk of ‘thinking aloud’ because that is often what we do: in many cases, our thoughts become choate only through their expression” (*supra* note 190 at para 108).
of thought at all – its predecessor, the 1960 *Canadian Bill of Rights,*\(^{353}\) only contains a reference to “freedom of speech” at s. 1(d) with no mention of thinking whatsoever.

The second reason why freedom of thought (as opposed to expression) seems to get little treatment 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”\(^{354}\) and the possibility of somehow 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 reflected in Peter W. Hogg’s overview of s. 2(b), where he outlines that the “references to ‘thought, belief, opinion’ will have little impact, since even a totalitarian state cannot suppress unexpressed ideas,” adding that “it is the reference to ‘expression’ in s. 2(b) that is the critical one, and the word expression is very broad.”\(^{355}\) Certainly, it is no doubt correct that the expression piece of s. 2(b) gets more play in constitutional litigation, but the right to think, as well as speak, freely has taken on greater significance its own right in this “golden age of surveillance.”\(^{356}\) The mental and existential state described by Richards as “intellectual privacy,”\(^{357}\) one’s ability to think without limits has come under attack in recent years, a development which has of late made this component of s. 2(b) more relevant and given it “impact.” Having been overshadowed by free speech since first

---

\(^{353}\) *Canadian Bill of Rights*, SC 1960, c 44, s 1(d).

\(^{354}\) *Supra* note 223 at 6.

\(^{355}\) *Supra* note 32 at 43-7. J B Bury, in *A History of Freedom of Thought* (Oxford: Oxford University Press, 1952), is likewise of the view that one “can never been hindered from thinking what he chooses so long as he conceals what he thinks” (at 1).

\(^{356}\) *Global Information Society Watch, supra* note 339 at 10.

\(^{357}\) *Supra* note 11 at 5.
debuting on the Canadian constitutional stage in 1982, the freedom of thought guarantee might now be gearing up for its own close-up.\textsuperscript{358}

While the s. 2(b) jurisprudence is almost exclusively focused on free speech, Canadian courts have on occasion considered freedom of thought as well and, in doing so, have emphasized the privacy element of this right. In \emph{Taylor}, for instance, Dickson C.J.C. acknowledges that “the freedoms of conscience, thought and belief are particularly engaged in a private setting,”\textsuperscript{359} a comment repeated verbatim by McLachlin C.J.C. in \emph{Sharpe}.\textsuperscript{360} 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”\textsuperscript{361} is central to s. 2(b) and forms an “extension of individual liberty.”\textsuperscript{362} Another forceful endorsement of this facet of s. 2(b), and the need to shelter ideas from public scrutiny, is found in \emph{R. v. Watts}, where the Provincial Court

\begin{footnotesize}
\begin{itemize}
  \item[358] This tendency by Canadian courts to emphasize free speech over freedom of thought is telescoped by Dickson C.J.C. in \emph{R v Andrews}, [1990] 3 SCR 870 at para 14, 77 DLR (4th) 128, where 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.” Richards traces a similar neglect of freedom of thought in the U.S. context: “If we're interested in the creation of new ideas, we should want people to experiment with controversial ideas. But this notion has not been deeply developed in First Amendment law or theory...discussions of free speech have only rarely addressed the question of how we ensure that new and interesting ideas get generated” (\textit{supra} note 11 at 98).
  \item[359] \textit{Supra} note 187 at para 77.
  \item[360] \textit{Supra} note 190 at para 26. In \emph{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.”
  \item[361] \textit{Retail, Wholesale and Department Store Union, Local 558 v Pepsi-Cola Canada Beverages (West) Ltd.}, 2002 SCC 8 at para 32, [2002] 1 SCR 156.
  \item[362] \textit{Lavigne v Ontario Public Service Employees Union}, [1991] 2 SCR 211 at para 116, 81 DLR (4th) 545 (quoting the trial judge).
\end{itemize}
\end{footnotesize}
of British Columbia celebrates the possibility of private thought. Angelomatis J. asks: “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.” For him, it is “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.”

So why is freedom of thought, formerly not given much attention in the case law, suddenly relevant in the surveillance context? The answer, as suggested above, is that technological advances have rendered the once seemingly impossible task of reading minds less fantasy and more reality, as online data trails expose our thoughts and desires for state (and corporate) consumption. Richards isolates this 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.” As he discerns, while “in the past, access to ideas has come principally from print media,” today such access is web-based so that “gradually, over the decades, technologies have come to mediate our thinking, reading, and communications.” Cockfield too is alert to this new normal, warning that while “governments

---

364 Ibid at para 10. This insistence on the primacy of private thought is reflected in the child pornography exemptions carved out of s 163.1(4) of the Criminal Code by McLachlin C.J.C. in Sharpe and recalls her assertions in that case that “it is a fine line that separates a state attempt to control the private possession of self-created expressive materials from a state attempt to control thought or opinion” and that “[t]o ban the possession of our own private musings thus falls perilously close to criminalizing the mere articulation of thought” (supra note 190 at para 108).
365 Supra note 11 at 96.
366 Ibid at 175.
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.”

And, 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.”

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.” This statement is particularly apropos in light of current concerns over government surveillance, and rings true across any jurisdiction in which this manner of privacy invasion is a problem. While it might once have been a truism that speech, not thought, could be caught by the state’s monitoring apparatus, technological developments, in combination with post-9/11 political malaise, have ignited a perfect storm in which one’s private musings are themselves no longer safe. Kaye, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, is himself careful in a 2015 report to bring this state of affairs to the attention of the Human Rights Council. Insisting

---

367 Arthur J Cockfield, “Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance” (2003) 29 Queen's LJ 364 at 395. Jeffrey Rosen, in The Unwanted Gaze: The Destruction of Privacy in America (New York: Random House, 2000), paints this new reality: “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” (at 7).

368 Ibid.

369 Ibid at 103.
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.”

“Targeted 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.”

As well as speech issues resulting from online surveillance, then, the privacy aspect of s. 2(b)
could prove helpful with respect to any freedom of thought violation. This might even be doubly
so, one could argue, given the two privacy layers pierced through this type of breach: the
storming of our online world and the resulting interference with mental activities usually defined
by the courts in terms of their private character. Particularly given the rise of our surveillance
culture, s. 2(b) could serve double duty in this regard, as those deterred from surfing as well as
speaking could add this Charter provision to their constitutional tool kit. Sometimes, despite the
popular saying, more is more, and it is difficult to understand how expanding the range of legal
responses in Canada to this 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 in the
concluding section of this chapter, that the CCLA, CJFE and BCCLA have evinced faith in this
approach by featuring it in legal challenges to aspects of the ATA 2001 and ATA 2015. Turning
to review these proceedings and to parse the strengths of and potential evidentiary issues raised

370 Supra note 109 at para 21.
371 Ibid.
by this particular use of s. 2(b), I will document how this strategy is reflected in current s. 2(b) litigation and offer suggestions on ways in which to maximize its effectiveness in the courtroom.

4 From concept to courtroom

4.1 Two cases featuring a privacy-centric vision of s. 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 this or that approach to submit them to judicial scrutiny. One of the interesting features of cases like *Spencer*, *Sharpe* and *Taylor*, which isolate the intersection of speech and privacy, is that none of them actually involve, as far as one can discern, the use of s. 2(b) in the privacy-focused manner which I have explored above. *Spencer*, the most recent and arguably on point of these Supreme Court of Canada decisions, is actually a s. 8 proceeding and, despite its forward-looking and novel treatment of anonymity and freedom of expression, never formally considers s. 2(b) itself. This is remarkable, and leaves one searching for other “real life” scenarios in which this mixing of privacy and speech has been introduced in the courtroom and adjudicated by the bench. Having undertaken this search, I can advise that, with one exception detailed below, it is difficult to locate judgments passing verdict on this *Charter* strategy, an outcome likely flowing from the relatively recent nature of Bill C-51 and related statutory developments.

It is reasonable to assume that, as Canadians become aware of more of the same, legal proceedings will be commenced accordingly to stem the tide of invasive government action.

That said, while there exists little in the way of concluded litigation on point, two challenges (one comprising of two distinct proceedings) have been commenced which concretely illustrate how s. 2(b) can be creatively mobilized with a privacy focus to combat government online
surveillance. The July 2015 challenge to Bill C-51, initiated jointly by the CCLA and the CJFE,\textsuperscript{372} covers much legal ground in attacking five separate aspects of the omnibus statute. In addition to impugning SCISA and the nebulous \textit{Criminal Code} amendment relating to the “commission of terrorism,” the applicants target the \textit{Secure Air Travel Act} and changes via the \textit{ATA 2015} to the \textit{Immigration and Refugee Protection Act} and the \textit{CSIS Act}.\textsuperscript{373} As broadcast in a news release posted on the CCLA website, this lawsuit was commenced in the Ontario provincial court because of the “disturbing implications for free speech, privacy and the powers of government”\textsuperscript{374} presented by Bill C-51. According to Tom Henheffer, CJFE Executive Director, who is quoted in the bulletin, this statute “unjustifiably infringes on the rights of all Canadians without making our country any more secure, and must be struck down.”\textsuperscript{375} For her part, Sukanya Pillay, Executive Director of the CCLA, makes clear that this law is being opposed on the basis that it “creates broad and dangerous new powers, without commensurate accountability.”\textsuperscript{376}

While this proceeding has yet to advance to a hearing, certain aspects of its approach to s. 2(b) are evident from the Notice of Application, particularly as it relates to SCISA and the \textit{Criminal Code} amendments. Reviewing these two components of the pleading, one glimpses a more conventional use of s. 2(b) as well as its deployment in response to privacy breaches. Regarding the first, this concerns the introducing of s. 83.221 into the \textit{Criminal Code}, an offence tied to the

\begin{itemize}
\item \textsuperscript{372} July 21, 2015 Notice of Application, \textit{supra} note 203.
\item \textsuperscript{373} \textit{Ibid} at 3-4.
\item \textsuperscript{374} “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>.
\item \textsuperscript{375} \textit{Ibid}.
\item \textsuperscript{376} \textit{Ibid}.
\end{itemize}
communication, advocating or promotion of “terrorism offences in general,” which the applicants view as criminalizing “constitutionally protected speech and other expressive activities.”377 This more classic leveraging of s. 2(b) is supplemented, with respect to SCISA, with an argument based explicitly in a privacy framework. Taking issue with the breadth of the information sharing powers blessed by SCISA, the CCLA and CJFE avow that the “invasive state archiving and information sharing” between government departments will “deter” and “chill legitimate expression.”378 Such “secret” activity is characterized by the litigants in a way suggestive of the surveillance state and Bentham’s Panopticon, as those under observation are unable “to determine (or challenge in any meaningful way) how their activities and conduct have been construed …[or] shared and used”379 by Ottawa.

On April 1, 2014, more than a year prior to the coming into force of Bill C-51 and the start of the CCLA/CJFE litigation, the BCCLA commenced a class action challenging ss. 273.65, 273.68 and 273.7 of the National Defence Act,380 provisions relating to CSE surveillance efforts.381 Later that year, the BCCLA initiated a second proceeding, similar in scope to its first case but packaged as a standard action and dropping any reference to s. 273.7.382 Central to both claims, advanced on the basis of ss. 2(b) and 8 of the Charter, are the CSE powers granted by s. 273.65

377 Supra note 203 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).
378 Ibid at para 34.
379 Ibid at paras 34-35.
to “intercept private communications.”  As stipulated in the act, 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.”

Regarding the former, s. 273.65(2) requires that any CSE interception must be “directed at foreign entities located outside of Canada” and can only be “used or retained if they are essential to international affairs, defence or security.”

Ministerial authorizations are needed to engage in this stealth monitoring activity, though s. 273.68 is vague on timelines or the possibility of multiple renewals, other than the statement that “no authorization or renewal may be for a period longer than one year.”

According to the BCCLA’s October 27, 2014 Statement of Claim, the “Minister issued at least 78 Authorizations between 2002 and 2012.”

The constitutional arguments raised by the BCCLA in the April and October 2014 proceedings are nearly identical and neatly foreground the privacy implications stemming from this interception of online communications. In impugning ss. 273.65 and 273.68, introduced into the National Defence Act through the ATA 2001, interference with the private sphere is front and centre, an issue addressed not merely through s. 8 but equally by means of s. 2(b). As announced by the BCCLA in its October 2014 Statement of Claim, the “impugned provisions and Authorizations that purport to provide CSEC with legal authority to intercept the private communications of persons in Canada are an infringement of s. 2(b).”

---

383 *National Defence Act, supra* note 380 at s 273.65(1), (3).
385 *Ibid* at s 273.65(2).
386 *Ibid* at s 273.68(1).
387 *Supra* note 382 at para 26.
applicant’s use of s. 8, on the basis of which this surveillance power is attacked as violating “reasonable expectation[s]” regarding the use and dissemination of personal information, the right to free speech is vital to this challenge. Further, as well as simply applying to the interception of expression, s. 2(b) is likewise enlisted in response to CSE efforts to “collect, analyze, retain, use and/or distribute internationally metadata that is associated with or produced by persons in Canada.” In invoking s. 2(b) in terms of information sharing in addition to private speech, these BCCLA lawsuits (like the CCLA/CJFE litigation) reflect the breadth of privacy-related possibilities attaching to this Charter right.

Currently, the CCLA/CJFE and BCCLA proceedings, which signal the ample possibilities latent within s. 2(b), are ongoing and it is impossible to predict (i) if they will make it to a hearing and, if so, (ii) how their privacy-centric free speech arguments will be received by the courts. At minimum, it would appear that, based on the available information, this trinity of cases continues to move forward on their respective tracks, even making the occasional headline along the way. Whatever their outcome, these matters are illustrative of a recent development in national security Charter litigation in which s. 2(b) is pleaded in response to the chilling effects of surveillance and related information sharing activities. Moreover, while the statutory provisions opposed by the litigants are not limited to online personal information and communication, these three challenges, to a lesser or greater extent, glance at the internet.

---

389 Ibid at para 39.
390 One of the BCCLA cases was in the news in the summer of 2016 in connection with the Crown’s alleged efforts to suppress information concerning CSE surveillance practices, including the nature and extent of intercepted metadata. See Sunny Dhillon, “B.C. advocacy group decries document redactions in federal spying case”, Globe and Mail (23 June 2016), online: <http://www.theglobeandmail.com/news/british-columbia/bc-advocacy-group-says-documents-needed-for-case-were-heavily-redacted/article30601575/>. 
dimension of state surveillance which continues to captivate Canadians. Though the CCLA/CJFE Notice of Application does not explicitly mention the web (other than speaking of Criminal Code “internet deletion provisions”), its reference to the “era of ‘big data’ information processing” with respect to 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 s. 2(b).” Together, such lawsuits point to an expanded potential for the free speech guarantee, a contemporary reading of this right responsive to our privacy perils in cyberspace.

4.2 Advantages and potential challenges in the courtroom

Whatever the results of the CCLA/CJFE and BCCLA litigation, I suggest that there is at least one major procedural advantage to s. 2(b), as compared to s. 8, that should be considered when framing a Charter challenge to privacy-invasive provisions like those in SCISA and the National Defence Act. Determining in such cases whether to rely on one or both of these grounds will hinge on a constellation of factors, including most simply the existence or absence of a freedom of expression problem. Assuming that expression and, accordingly, s. 2(b) are in play, one might wish to plead free speech since doing so will avoid the meddlesome reasonable expectation of privacy test at the centre of s. 8. Whereas s. 2(b) violations are often conceded by the Crown, thus reversing the onus and kicking the fight over to s. 1, parties seeking to show an illegal

391 Supra note 203 at para 9.
392 Ibid at para 35.
393 Supra note 381 at para 45; supra note 382 at para 37.
394 Given that privacy is far more often referenced in terms of s. 8 than s. 7 of the Charter, I shall restrict my comments on point to ss 2(b) and 8.
395 As explained by Hogg, supra note 32 at 43-6: “the unqualified language of s. 2(b), reinforced by the broad interpretation that has been given to that language, means that, in most of the freedom of expression cases, it is easy to decide that, yes, the impugned law does limit s. 2(b).”
search must first cross this hurdle before the government is forced to defend its actions and/or laws. In addition to expanding the range of privacy-related concerns open to attack to include speech violations, then, this use of s. 2(b) likewise affords a significant structural benefit to the moving party. Perhaps ideally, facts permitting, one could advance ss. 2(b) and 8 together, allowing for a two-prong approach (search and seizure and speech) while, on one of these tracks at least, ducking the reasonable expectation analysis.

Central to this s. 8 threshold is the concept of consent and the extent to which, in revealing personal information to a third party, one could reasonably be said to have granted this party permission to further disclose these details to other persons or organizations. Additionally, depending on one’s actions (e.g. opening a suitcase in public such that its contents are displayed for all to see), consent to disclose otherwise private data might be inferred, even in the absence of any explicit agreement to this effect. These issues are complex, and rendered even more problematic by the multitude of disclosure clauses buried in the avalanche of standard form contracts that we are basically required to enter into if we want to remain on the grid. While Canadian courts have rejected the U.S. “risk analysis” approach to the Fourth Amendment, whereby “allowing others into a zone of personal privacy” will “forfeit a claim that the state is

_________________________

It is not unusual for government respondents to concede s. 2(b) violations, thus triggering the s. 1 analysis. Such was the case in Sharpe, for instance, where the “Crown concedes that s. 163.1(4)’s prohibition on the possession of child pornography infringes the guarantee of freedom of expression in s. 2(b) of the Charter” and the only outstanding “issue is whether this limitation of freedom of expression is justifiable under s. 1” (supra note 190 at para. 5). For a more recent concession by the government that the impugned law at issue violates s. 2(b) see, for instance, Saskatchewan (Human Rights Tribunal) v Whatcott, 2013 SCC 11 at para 62, [2013] 1 SCR 467.
excluded from that same zone,” these clauses can still prove vexing. As Mark MacAulay
imparts: “Consumers are often ignorant of the complicated mechanisms allowing for disclosure
of their information,” a fact leading them to “sign contracts and live under the yoke of legislation
not because they agree to the substance of these frameworks but because they have no other
meaningful choice.” Or, as noted by Philippa Lawson and Mary O’Donoghue: “we caution
against too much reliance on consent, given that its exercise is often more notional than real.”

The situation has become thornier still in the internet age as courts have struggled with a host of
novel issues, including the extent to which internet service providers can disclose to the
authorities personal subscriber information and the privacy status of metadata. This reality is
underscored by Teresa Scassa, Jennifer A. Chandler and Elizabeth F. Judge, who pronounce that
the “interplay between s. 8…and data protection legislation has come into sharp focus in recent
cases involving the extent to which data protection legislation creates a reasonable expectation of

---


397 Mark MacAulay, “Contracts, Legislative Frameworks and the Reasonable Expectation of Privacy: Rethinking Section 8 in the Service Provision Context” (2015) 20 Can Crim L Rev 111 at 113-114. He adds: “It is probably beyond serious debate, in light not only of *Spencer* but of decades of preceding case law to this effect, that contracts and legislation can and do matter to the threshold section 8 inquiry” (at 125).


399 In addition to *Spencer*, such issues have recently been addressed by the Court of Appeal for Ontario in *Ward, supra* note 170, and the Saskatchewan Court of Appeal in *R v Trapp*, 2011 SKCA 143, 377 Sask R 246. See Slane, *supra* note 396 for an analysis of this development in the case law, though it should be noted that because her article preceded Cromwell J.’s 2014 decision in *Spencer* Slane’s discussion is restricted to the 2012 Saskatchewan Court of Appeal judgement in this case. See also MacAulay, *supra* note 397.
privacy in certain data.” According to some, this confusion has not been remedied by the
Spencer ruling, which in MacAulay’s view “has left the ambiguities of the reasonable
expectation of privacy intact” and has “conceivably left the door open to future intrusions on
customer privacy through the operation of unfair contracts and potentially abusive legislation and
regulation.” Given this ongoing state of uncertainty, addressing privacy concerns by means of
s. 2(b), especially in the context of online communications, would obviate the need to roll the
dice as to whether one was deemed to possess a reasonable expectation of privacy in such
information. For the time being at least, until the courts succeed in further nailing down these
principles, the freedom of expression right presents a helpful alternative (or additional)
constitutional weapon in the fight against surveillance.

Beyond this procedural advantage, the use of s. 2(b) in response to privacy invasions would
bring to the fore the expression aspect of the privacy interest, which given the prominence of s. 8
in this context risks being reduced to a debate over reasonable expectations alone. While the
connections between privacy and s. 8 are well established, it is easy to forget that such
expectations are not the whole story and that other important values, including speech, remain
relevant here. Particularly in light of the definitional flexibility explored above, one can imagine
privacy-related violations under s. 2(b) (or s. 7) even where one cannot meet this s. 8 threshold.
This could become relevant at the final stage of the Oakes test, such that even if an impugned

400 Teresa Scassa, Jennifer A Chandler & Elizabeth F Judge, “Privacy by the Wayside: The New
Information Superhighway, Data Privacy, and the Deployment of Intelligent Transportation
Systems” (2011) 74 Sask L Rev 117 at 134-135. See also Teresa Scassa & Anca Sattler,
“Location-Based Services and Privacy” (2011) 9 CJLT 99 at 133-134.
401 Supra note 397 at 113.
402 Oakes, supra note 22.
law was found to be perfectly proportional up to and including minimal impairment, one could still argue that its impact on free speech was sufficient to tip the balance at this final phase of the s. 1 analysis. As has been recently stressed by the Supreme Court of Canada in *R. v. K.R.J.*, this balancing of deleterious and salutary effects captures the “essence of the proportionality enquiry” since “it is only [here] that courts can transcend the law’s purpose and engage in a robust examination of the law’s impact on Canada’s free and democratic society ‘in direct and explicit terms.’”\(^{403}\) Thus focused on broader notions of democracy and freedom, this “normative”\(^ {404}\) assessment is ideally suited for arguments relating to the primacy of the s. 2(b) guarantee.

Just as a privacy-oriented reading of s. 2(b) offers these advantages, however, so too does it present a potential challenge for litigants which, though far from a deal-breaker, will need to be confronted in the planning stages of litigation. Put simply, those alleging that government surveillance, actual or suspected, is responsible for chilling thought or speech will need to remain alert to how best to prove this cause and effect in court. This issue was determinative in an earlier CCLA proceeding focused on the intersection of speech and privacy, where CSIS surveillance powers outlined in the *CSIS Act* were attacked on the basis of s. 2(b). Central to this case was the claim that “intrusive surveillance techniques and other such powers have a ‘chilling effect’ on the willingness of citizens to exercise their right to engage in lawful advocacy, protest or dissent.”\(^ {405}\) Anticipating the BCCLA response to ss. 273.65 and 273.68 of the *National Defence Act*, and recalling the anxiety-provoking worlds of Bentham and Orwell, the CCLA took

\(^{403}\) *R v KRI*, 2016 SCC 31 at para 79.

\(^{404}\) *Ibid*. Regarding the significance and distinct nature of this final step of the *Oakes* test see also McLachlin C.J.C.’s analysis in *Hutterian Brethren*, *supra* note 33 at paras 72-78.

\(^{405}\) *Corporation of the Canadian Civil Liberties Association v Attorney General of Canada*, 74 OR (2d) 609, [1990] OJ No 1481 (QL) at para 19 (HCJ).
exception with the “surreptitious” and “covert” nature of CSIS monitoring activities. As paraphrased by Potts J. at the Ontario High Court of Justice, those participating 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.”

From the perspective of Potts J. and, subsequently, the Court of Appeal for Ontario, this challenge was doomed by a deficiency in the evidence (the Court of Appeal also found that the CCLA should not have been granted public interest standing). Charron J.A., writing for the majority of the Court of Appeal, and having reviewed the affidavits adduced by the CCLA, inventories several problems, including a focus on overt, not covert, surveillance, vague allegations and reliance upon “personal opinion and argument.” While Abella J.A., writing in dissent, concurs regarding the “inability of C.C.L.A. to provide an evidentiary basis,” however, she is quick to defend the potential merits of this s. 2(b) counterpunch to intrusive CSIS practices. She opines: “The information contained in the 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 C.S.I.S. Act.” Additionally, despite acknowledging the weakness of the record, she suggests that government surveillance can cause violations of s. 2(b) and that the CCLA did adduce some

406 Ibid at para 4.
407 Ibid at para 19.
408 Corporation of the Canadian Civil Liberties Association v Attorney General of Canada, 40 OR (3d) 489, [1998] OJ No 2856 at paras 44-72 (QL) (CA) [CCLA].
409 Ibid at para 109.
410 Ibid at para 103.
(though, apparently, not enough) evidence to this effect. “There is no question,” Abella J.A. delineates, “that the perception of C.S.I.S. intervention was, to say the least, unsettling to the people involved and potentially inhibiting.”

While this particular CCLA claim foundered on evidentiary grounds, the Court of Appeal decision (and the two lower court judgments of Potts J.) provide valuable insight into strategies for avoiding litigation pitfalls of the sort canvassed by Charron J.A. Critically, Charron J.A. does not indicate that the chilling of thought or expression can never be proven, but merely points to the “lack of an evidentiary basis” in this instance. Further clarity on the type of evidence required to make out a chill on s. 2(b) rights is offered by the Court of Appeal in R. v. Khawaja, where it proposes that, “at the very least,” such a violation would call for “credible anecdotal evidence” or “credible expert evidence.” Using these and similar judicial pronouncements as a roadmap, moving parties will need to prepare their cases accordingly in order to take full advantage of s. 2(b) in challenging privacy-invasive government action. Doing so would allow litigants to maximize the potential of this constitutional argument and broaden their attack on unwanted monitoring. Should Ottawa introduce more legislation in the mold of Bill C-51, and should Canadians continue to bristle under an unwanted gaze, it can be assumed

411 Ibid.
412 Ibid at para 83.
413 R v Khawaja, 2010 ONCA 862 at para 122, 103 OR (3d) 321 (see, more broadly, paras 118-135 of this ruling). The Supreme Court of Canada, in upholding the Court of Appeal decision, confirms this approach to the evidentiary requirements needed to prove a chilling of s. 2(b) rights. See R v Khawaja, 2012 SCC 69 at paras 78-83, [2012] 3 SCR 555. As McLachlin C.J.C. highlights, however, such requirements will differ depending on the legislation or government action at issue. On this point see also St. Elizabeth Home Society v Hamilton (City), 2008 ONCA 182 at paras 31-34, 89 OR (3d) 81. For an analysis of chilling effect principles, largely from the U.S. perspective, see Sunny Skye Hughes, supra note 340.
that the speech-privacy nexus will continue to thrive as advocates test the limits of the surveillance state.

5 Conclusion

In this chapter I have traced the connections between privacy and expression and have demonstrated how this link has been identified by Canadian courts and adopted by civil society groups in s. 2(b) litigation targeting government surveillance. This highlighting of the privacy dimension informing the free speech guarantee is particularly timely, I have detailed, given our slavish connection to the internet and the ease with which both our thoughts and speech can now be intercepted online. Responding to this twenty-first century threat, which has gripped the popular imagination, advocates have taken hold of this vision of s. 2(b) in their fight against such invasions of the private sphere. As Abella J.A. asserts in relation to the CCLA’s fight against CSIS monitoring tools: “It goes to the heart of an open democracy that members of the public are, and perceive that they are, free from unwanted government surveillance when they are engaging in lawful, even if provocative activity.”414 While this specific case may not technically have been a win for the CCLA, its forceful attack on CSIS’s “exceptional legislative tool”415 set the stage for future challenges, including the ongoing BCCLA and CCLA/CJFE lawsuits referenced above. And, as concerns regarding state snooping continue to grow in our post-9/11 reality (the Court of Appeal rendered its CCLA decision in 1998), it seems likely that judges will remain ever more mindful of digital privacy.

414 CCLA, supra note 408 at para 104.
415 Ibid.
Time will tell, as it always does, whether Bill C-51 represents a low watermark in recent Canadian legislative efforts or if it constitutes merely the first gambit in the ongoing development of federal surveillance powers. The Trudeau government, since capturing a majority government in October 2015, has yet to take real steps toward repealing any part of the *ATA 2015*, despite its promise to do so. As exclaimed on the Liberal Party website: “We will repeal the problematic aspects of Bill C-51, and introduce new legislation that better balances our collective security with our rights and freedoms.”\(^{416}\) Among the list of eight priorities pledged in this context, one is told 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.”\(^{417}\) Though certainly a start, the value of some of these commitments remains an open question. Forsese and Roach have shown that judicial warrants can prove less rather than more helpful in this regard,\(^{418}\) and at least some in the press have criticized the committee process (the only plank of this platform on which Ottawa has acted thus far).\(^{419}\) In the meantime, one can take comfort in the expanding reach of s.

\(^{416}\) Official Liberal Party of Canada 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*, which declares: “The Government is aware that its actions in security matters can impact rights. 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” (*supra* note 225 at 6).

\(^{417}\) *Ibid.* And, in addition to these promises, the *Green Paper* invites Canadians to “respond online at Canada.ca/national-security-consultation to the issues raised in this” background document and advises that the “Government will consider the responses and use them to help develop any new laws and policies” (*supra* note 225 at 7).

\(^{418}\) *Supra* note 7 at 353-354, 392, 506.

\(^{419}\) See Lawrence Martin, “Anti-terrorism law: Why the Liberals aren’t living up to vow to amend it”, *Globe and Mail* (2 August 2016), online: <http://www.theglobeandmail.com/opinion/bill-c-51-why-the-liberals-arent-living-up-to-promises-to-amend-the-law/article31220198/>; Thomas Walkom, “Justin Trudeau’s near-
2(b) and other constitutional tools, which remain poised to defend our privacy and other liberties against whatever might lie ahead.

CONCLUSION

In this thesis I have attempted to contribute to current debates, within and beyond the courtroom and academia, concerning national security, state surveillance of online personal information and the limits of the private sphere. As I have discussed, governments, in seeking to root out terrorism and other evils, have in certain instances crossed a line, state behaviour which has in turn placed our civil liberties in peril. This is not, of course, an original insight, and has been documented with increasing frequency over the last number of years, particularly post-9/11 and the Snowden leaks. In Canada, as I have explained, the source of much recent concern in connection with this overstepping by Parliament has been the ATA 2015 and its creation of legislation like SCISA and the s.83.221 Criminal Code crime of promoting “terrorism offences in general.”\textsuperscript{420} And, prior to the ATA 2015, Canadians had to contend with the ATA 2001, which likewise compromised privacy online and elsewhere through, for instance, its amendments to the National Defence Act.\textsuperscript{421} These laws, and the clear and present danger they represent, have caused many legal experts to ring the death knell of internet privacy in Canada and have, as detailed in the preceding pages, triggered a number of lawsuits targeting such surveillance excess.

In focusing on the intersection of freedom of expression and privacy, I have situated my arguments within the context of what I refer to above as this “grave new world” of government surveillance and declining civil liberties. I have argued that, given this move by Ottawa toward increased information monitoring and sharing, it behooves Canadians to identify and use as

\textsuperscript{420} Criminal Code, s 83.221(1).
\textsuperscript{421} National Defence Act, RSC, 1985, c N-5, ss 273.65, 273.68.
many constitutional tools as possible in defending against unwarranted privacy invasion. Section 2(b) constitutes one such tool, I suggest, and should where appropriate be interpreted and applied in a privacy framework. While this reading of the free speech guarantee runs contrary to the traditional view of speech and privacy, which paints them as antithetical interests, I outline two developments which confirm the legitimacy of this alternative conceptual approach. First, I demonstrate how the Supreme Court of Canada and other courts have already accepted the complementarity of these rights, a viewpoint articulated most recently in *Spencer*. Second, I inventory the ways in which the CCLA/CJFE and BCCLA lawsuits, *Charter* challenges relating to the *ATA 2015* and the *ATA 2001* respectively, rely in part on this privacy-centric vision of s. 2(b). In other words, although I stress that, as compared to ss. 7 and 8, s. 2(b) has received limited attention in privacy analyses, I make clear that, in practice, this perspective on s. 2(b) features both in jurisprudence and in high profile cases currently before Canadian courts.

And what of next steps in the struggle for online privacy, particularly assuming that the Trudeau government continues to drag its heels on Bill C-51 and similar files? This would at present appear to be a safe assumption, given Ottawa’s continued hedging over Bill C-51 and its noticeable lack of progress on this front. Accordingly, it seems likely that Canadians will be saddled with these issues for some time to come, a reality which will continue to inform public discourse and litigation strategy alike. Beyond the tried and tested constitutional strategies, it will remain critical for advocates to push the *Charter* boundaries in attacking the method and substance of government surveillance. Thus while more traditional arguments (including s. 8 and the language of reasonable expectations) will continue to make sense in many factual scenarios, less conventional approaches, like the fusing of privacy and freedom of expression,
will likewise facilitate victories in this fight for online liberty and may loom large at the final stage of the s. 1 analysis. Especially today, when our speech and thoughts depend more than ever on the internet, it is essential that we defend such liberty in as robust a manner as possible. The nexus of speech and privacy studied in this thesis represents, I submit, a welcome step forward in this process, and will hopefully open the door to other equally novel constitutional devices in the weeks, months and years ahead.
BIBLIOGRAPHY

LEGISLATION

i) Canadian legislation

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

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

*Canadian Bill of Rights*, SC 1960, c 44


*Canadian Security Intelligence Service Act*, RSC, 1985, c C-23

*Criminal Code of Canada*, RSC, 1985, c C-46

*Freedom of Information and Protection of Privacy Act*, RSO 1990, c F-31


*National Defence Act*, RSC, 1985, c N-5

*Personal Information Protection and Electronic Documents Act*, SC 2000, c 5

*Privacy Act*, RSC, 1985, c P-21

*Security of Canada Information Sharing Act*, SC 2015, c 20

ii) International legislation

California Senate Bill No 568, c 336, 22581(a)(1), online: <http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568>

*Constitution of Brazil*, 5 October 1988, title II, c I


*Ordinance for the Regulating of Printing*, online: <http://www.british-history.ac.uk/noseries/acts-ordinances-interregnum/pp184-186>
JURISPRUDENCE

i) Canadian jurisprudence

Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401, 2013 SCC 62, [2013] 3 SCR 733

Alberta v Hutterian Brethren of Wilson Colony, 2009 SCC 37, [2009] 2 SCR 567

AM v Ryan, [1997] 1 SCR 157, 143 DLR (4th) 1


Baier v Alberta, 2007 SCC 31, [2007] 2 SCR 673


B (R) v Children’s Aid Society of Metropolitan Toronto, [1995] 1 SCR 315, 122 DLR (4th) 1

Canada (Attorney General) v Hislop, [2007] 1 SCR 429, 278 DLR (4th) 385

Canada (Human Rights Commission) v Taylor, [1990] 3 SCR 892, 75 DLR (4th) 577


Corporation of the Canadian Civil Liberties Association v Attorney General of Canada, 74 OR (2d) 609, [1990] OJ No 1481 (QL) (HCJ)

Corporation of the Canadian Civil Liberties Association v Attorney General of Canada, 40 OR (3d) 489, [1998] OJ No 2856 (QL) (CA)


Dagenais v Canadian Broadcasting Corp, [1994] 3 SCR 835, 120 DLR (4th) 12

Dagg v Canada (Minister of Finance), [1997] 2 SCR 403, 148 DLR (4th) 385

Edmonton Journal v Alberta (Attorney General), [1989] 2 SCR 1326, 64 DLR (4th) 577


Germany (Federal Republic) v Ebke, 2001 NWTSC 17, 203 DLR (4th) 415

Godbout v Longueuil (City), [1997] 3 SCR 844, 152 DLR (4th) 577
Grant v Torstar Corp., 2009 SCC 61, [2009] 3 SCR 640


Hill v Church of Scientology of Toronto, [1995] 2 SCR 1130, 126 DLR (4th) 129

Hunter v Southam Inc., [1984] 2 SCR 145, 11 DLR (4th) 641

Irwin Toy Ltd. v Québec (Attorney General), [1989] 1 SCR 927, 58 DLR (4th) 577

Jane Doe 464533 v ND, 2016 ONSC 541

Jones v Tsige, 2012 ONCA 32, 108 OR (3d) 241

King v Power, 2015 NLTD(G) 32, [2015] NJ No 78 (QL)


Lavigne v Ontario Public Service Employees Union, [1991] 2 SCR 211, 81 DLR (4th) 545

McKinney v University of Guelph, [1990] 3 SCR 229, 76 DLR (4th) 545

Niemela v Malamas, 2015 BCSC 1024

Retail, Wholesale and Department Store Union, Local 558 v Pepsi-Cola Canada Beverages (West) Ltd., 2002 SCC 8, [2002] 1 SCR 156

Ruby v Canada (Solicitor General), 2002 SCC 75, [2002] 4 SCR 3

R v Andrews, [1990] 3 SCR 870, 77 DLR (4th) 128

R v Beare; R v Higgins, [1988] 2 SCR 387, 55 DLR (4th) 481

R v Bengert, Robertson (No. 8), 15 CR (3d) 37, [1979] BCJ No 1709 (SC) (QL)


R v Duarte, [1990] 1 SCR 30, 65 DLR (4th) 240

R v Dyment, [1988] 2 SCR 417, 55 DLR (4th) 503

R v Gomboc, 2010 SCC 55, [2010] 3 SCR 211

R v Khawaja, 2010 ONCA 862, 103 OR (3d) 321
R v Khawaja, 2012 SCC 69, [2012] 3 SCR 555
R v KRJ, 2016 SCC 31
R v Mentuck, [2001] 3 SCR 442, 205 DLR (4th) 512
R v Morgentaler, [1988] 1 SCR 30, 44 DLR (4th) 385
R v Oakes, [1986] 1 SCR 103, 26 DLR (4th) 200
R v O’Connor, [1995] 4 SCR 411, 130 DLR (4th) 235
R v Rowbotham, 11 CRR 302, 42 CR (3d) 164
R v Sharpe, 69 DLR (4th) 536, [1999] BCJ No 54 (QL)
R v Sharpe, 2001 SCC 2, [2001] 1 SCR 45
R v Spencer, 2014 SCC 43, [2014] 2 SCR 212
R v Stillman, [1997] 1 SCR 607, 144 DLR (4th) 193
R v Suberu, 2009 SCC 33, [2009] 2 SCR 460
R v Trapp, 2011 SKCA 143, 377 Sask R 246
R v Ward, 2012 ONCA 660, 112 OR (3d) 321
R v Wong, 56 CR (3d) 352, 1987 CarswellOnt 88 (WL Can)
Saskatchewan (Human Rights Tribunal) v Whatcott, 2013 SCC 11, [2013] 1 SCR 467
St. Elizabeth Home Society v Hamilton (City), 2008 ONCA 182, 89 OR (3d) 81
Suresh v Canada (Minister of Citizenship and Immigration), 2002 SCC 1, [2002] 1 SCR 3
Warman v Wilkins-Fournier, 2010 ONSC 2126, 100 OR (3d) 648 (Div Ct)
ii) International jurisprudence


**SECONDARY MATERIALS: INTERNATIONAL AGREEMENTS**

i) United Nations international agreements

*International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171


ii) Other international agreements

*American Convention on Human Rights*, 22 November 1969, 1144 UNTS 143


**SECONDARY MATERIALS: BOOKS**


Karanicolas, Michael, "Understanding the Internet as a Human Right" (2012) 10 CJLT 263


Richardson, Janice, *Law and the Philosophy of Privacy* (New York: Routledge, 2016)


**SECONDARY MATERIALS: ARTICLES AND ESSAYS**


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


Iacobucci, The Honourable Frank, "Recent Developments Concerning Freedom of Speech and Privacy in the Context of Global Communications Technology" (1999) 48 UNBLJ 189


Kozinski, Alex, “The Two Faces of Anonymity” (2015) 43 Cap U L Rev 1


MacKay, A Wayne, “Law as an Ally or Enemy in the War on Cyberbullying: Exploring the Contested Terrain of Privacy and Other Legal Concepts in the Age of Technology and Social Media” (2015) 66 UNBLJ 3

Mayeda, Graham, "My Neighbour's Kid Just Bought a Drone ... New Paradigms for Privacy Law in Canada" (2015) 35 NJCL 59


Roach, Kent, “CSEC’s Airport Program: Questions of Legality, Propriety and the Adequacy of Review” (2014) 60 Crim LQ 469


Scassa, Teresa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 CJLT 99


Sell, Saskia, “‘We are Anonymous.’ Anonymity in the Public Sphere: Challenges of Free and Open Communication”, online: (2013) 3:1 Global Media J, German ed, online: <http://www.db-thueringen.de/servlets/DerivateServlet/Derivate-27642/GMJ5_Sell_final.pdf>


Slane, Andrea, "Privacy and Civic Duty in R v Ward: The Right to Online Anonymity and the Charter-Compliant Scope of Voluntary Cooperation with Police Requests” (2013) 39 Queen's LJ 301


Streeter, Jeremy, “The 'Deception Exception': A New Approach to Section 2(b) Values and Its Impact on Defamation Law” (2003) 61 UT Fac L Rev 79

Strossen, Nadine, “Protecting Privacy and Free Speech in Cyberspace” (2001) 89 Geo LJ 2103


Whitman, James Q, “The Two Western Cultures of Privacy: Dignity versus Liberty” (2013) 113 Yale LJ 1151


SECONDARY MATERIALS: JOURNALISM AND BLOGS


Gilbert, David, “Right to be Forgotten – Google rejects 70% of 250,000 removal requests”, International Business Times (13 May 2015), online: <http://www.ibtimes.co.uk/right-be-forgotten-google-rejects-70-250000-removal-requests-1501029>


Kowalski, William, PEN Canada blog post (4 February 2015), online: <https://pencanada.ca/blog/does-cse-know-too-much-about-us>


Walker, Rob, “Recognizably Anonymous: How did a hacker group that rejects definition develop such a strong visual brand?”, Slate (8 December 2011), online: <http://www.slate.com/articles/arts/design/2011/12/guy_fawkes_mask_how_anonymous_hacker__group_created_a_powerful_visual_brand.html>


SECONDARY MATERIALS: REPORTS

i) Government of Canada reports


ii) United Nations reports


Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 23rd Sess, (17 April 2013), online: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement>


iii) Other reports


OTHER MATERIALS

i) Legislative history materials


ii) Court pleadings


iii) Miscellaneous materials


Constitute project, online: https://www.constituteproject.org

Electric Frontier Foundation, Surveillance Self-Defense project, online: <https://ssd.eff.org/en>

Canadian Bar Association website, online: <http://www.cba.org/Home>

Liberal Party of Canada website, online: <https://www.liberal.ca/realchange/bill-c-51/>

Sex Pistols, “I Wanna Be Me” (EMI Music Publishing Ltd., November 26, 1976)