The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference

Volume 71 (2015) Article 21

Towards a Public Law of Privacy: Meeting the Big Data Challenge

Lisa M. Austin

Citation Information

Austin, Lisa M.. "Towards a Public Law of Privacy: Meeting the Big Data Challenge." *The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference* 71. (2015).
http://digitalcommons.osgoode.yorku.ca/sclr/vol71/iss1/21

This Article is brought to you for free and open access by the Journals at Osgoode Digital Commons. It has been accepted for inclusion in The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference by an authorized editor of Osgoode Digital Commons.

Towards a Public Law of Privacy: Meeting the Big Data Challenge

Lisa M. Austin[*]

I. INTRODUCTION

Privacy law, to the extent that it regulates state information practices, wears two "public" hats. The first hat is constitutional law. For example, the Canadian *Charter of Rights and Freedoms*[1] protects privacy through protecting individuals against unreasonable searches and seizures. The second hat is public sector data protection law modelled on what are known as Fair Information Practices ("FIPs"). For example, in Canada the federal *Privacy Act*[2] regulates the collection, use and disclosure of personal information held by government institutions and provides individuals with a right of access to that information. We might say that the constitutional hat is concerned with state-individual relations in the context of law enforcement while the data protection hat is concerned with state-individual relations in the context of administering state programs. This article calls into question the ongoing relevance of this divide.

One of the strengths of the data protection law model is that it addresses the issue of privacy in relation to information *systems*. One of the big challenges facing Charter jurisprudence on privacy is that the constitutional framework is best suited to address privacy concerns associated with the state accessing a particular "bit" of information, not the way in which these bits are now being collected as parts of information systems that support new kinds of investigatory techniques. Consider, for example, some of the techniques that the Snowden

---

[*] University of Toronto Faculty of Law. Earlier versions of this article were presented at the 2014 Constitutional Cases Conference, April 10, 2015, Osgoode Hall Law School; at the "Surveillance and the Law" panel at Law and Society Association, Seattle, May 2015; and at the Privacy Discussion Forum, Paris, June 2015. I would like to thank the participants for their comments. I would also like to thank Julia Dryer for our discussions regarding s. 1 of the Charter. All errors remain mine.

[1] Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [hereinafter "Charter"].

[2] R.S.C. 1985, c. P-21.

revelations have highlighted, where large amounts of data about people who are not suspected of anything are collected in order to create analytic tools that allow for new forms of identification and targeting. If the Charter is going to face its "Big Data" moment, then it needs some of the resources of data protection law.

At the same time, data protection law does not have the resources to deal with the concern that is at the heart of section 8: the confrontation of the individual with the coercive power of the state. This is increasingly a problem given that Canada's *Privacy Act* is being pressed into service to protect privacy in the context of greater governmental information sharing for the purposes of national security. For example, Canada's new *Security of Canada Information Sharing Act*,[3] enacted by Bill C-51, dramatically increases information sharing between government institutions in order to facilitate "Big Data" techniques and the only privacy protections on offer are the government's claims that the *Privacy Act* continues to apply.[4] The problem is that in the data protection law model there are so many exceptions to the application of privacy protections in the context of both law enforcement and national security that it offers much weaker protection than the constitutional model of privacy protection. In order to inject constitutional considerations into the data protection law model, the Privacy Commissioner of Canada has called for an additional focus on necessity and proportionality, drawing upon the test from *R. v. Oakes*[5] to outline reasonable limits on rights.[6] However, this grafting of the *Oakes* test does not attend to the differences between the kind of balancing that takes place within the *Oakes* framework and that which takes place within section 8 of the Charter in determining whether an expectation of privacy is reasonable — differences which this article

---

[3] S.C. 2015, c. 20, s. 2.

[4] See Lisa M. Austin, "Anti-Terrorism's Privacy Sleight-of-Hand: Bill C-51 and the Erosion of Privacy" in Edward M. Iacobucci & Stephen J. Toope, eds., *After the Paris Attacks: Responses in Canada, Europe, and Around the Globe* (Toronto: University of Toronto Press, 2015) [hereinafter "Austin, 'Anti-Terrorism's Privacy'"]; Craig Forcese & Kent Roach, "Stumbling Toward Total Information Awareness: The Security of Canada Information Sharing Act" (2015) 12(7) Canadian Privacy L. Rev.

[5] [1986] S.C.J. No. 7, [1986] 1 S.C.R. 103 (S.C.C.) [hereinafter "*Oakes*"].

[6] Office of the Privacy Commissioner of Canada, *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada* (March 2011); These ideas of necessity and proportionality were also stressed by the Privacy Commissioner of Canada in his submissions on Bill C-51: "Submission to the Standing Committee on Public Safety and National Security of the House of Commons", Office of the Privacy Commissioner of Canada, March 5, 2015, online: <https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp>.

argues are important. It seems clear that if data protection law is going to offer meaningful privacy protection in relation to government information practices in the era of Big Data, then it needs some of the resources of the constitutional law of *privacy* and not just the constitutional law of reasonable limits on rights more generally.

The merging of these two frameworks is a large project to both undertake and defend. This article only purports to offer some initial reflections on a potential merger, focusing on recent Supreme Court cases, including *R. v. Spencer*,[7] *Wakeling v. United States of America*[8] and *R. v. Fearon*.[9] First, this article outlines some of the ways in which our Charter jurisprudence already adopts some of the insights that come out of the data protection law model and points to some of the ways in which this can be built upon. Next, the article outlines the potential problems of using data protection law framework in the context of law enforcement and anti-terrorism if the limitations of data protection are not well understood when balancing interests. Finally, it finishes with some proposals about how merging the two models might better address some new types of "Big Data" investigatory techniques, or, what we now all describe post-Snowden, collecting-the-haystack-to-find-the-needle.

II. PRIVACY AND INFORMATION SYSTEMS

The idea of informational privacy protected by both constitutional law and data protection law is remarkably similar in its abstract expression by Canadian courts and other legal decision makers. For example, the Supreme Court has accepted Westin's definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[10] This is also the definition often invoked by Canada's federal, provincial and territorial privacy commissioners when interpreting and discussing the data protection law regime.

---

[7] [2014] S.C.J. No. 43, [2014] 2 S.C.R. 212, 2014 SCC 43 (S.C.C.) [hereinafter "*Spencer*"].

[8] [2014] S.C.J. No. 72, [2014] 3 S.C.R. 549, 2014 SCC 72 (S.C.C.) [hereinafter "*Wakeling*"].

[9] [2014] S.C.J. No. 77, [2014] 3 S.C.R. 621 (S.C.C.) [hereinafter "*Fearon*"].

[10] *R. v. Quesnelle*, [2014] S.C.J. No. 46, 2014 S.C.R. 390, at para. 34 (S.C.C.); *R. v. Tessling*, [2004] S.C.J. No. 63, [2004] 3 S.C.R. 432, 2004 SCC 67, at para. 23 (S.C.C.); citing A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), at 7.

Despite this similarity, there is a big difference between the two frameworks. The concerns that prompted the adoption of data protection statutes such as the *Privacy Act* are well captured in the 1972 Canadian report of the Task Force on Privacy and Computers.[11] The focus was on computerized information systems and their acceleration of social trends towards every-increasing accumulation, centralization and distribution of data.[12] As the Task Force states, "[i]nformation systems — computerized or not — cannot themselves invade personal privacy, but their use almost inevitably entails it."[13] We need to read statutes like the *Privacy Act* from a systems perspective. The issue is not whether a particular "bit" of information collected is private information, the issue is how to protect privacy overall within a system that collects, uses and discloses so many "bits" of information. Therefore the threshold question of such regimes is whether something is "personal" information (defined as information about an identifiable individual) and not whether it is "private" information.

The focus of Charter jurisprudence in the area of informational privacy has been quite different, for many cases are centrally concerned with the question of whether a particular "bit" of information is private or not. The Charter is engaged only where there is a "reasonable expectation of privacy". Much of the Charter jurisprudence on privacy indicates that a reasonable expectation of privacy is much narrower in scope than personally identifiable information. For example, the Charter context is dominated by considerations such as whether the information at issue falls within one's "biographical core" or is "specific and meaningful".[14]

This Charter focus on the privacy of bits rather than the privacy of systems creates potential problems in assessing modern information surveillance techniques which have much in common with the information systems targeted by data protection law: many "bits" are collected in order to be put together and used in different ways; they are thought to raise privacy concerns but these concerns are not entirely about the "bits" themselves but how the system as a whole operates.[15] However, the recent

---

[11] Task Force on Privacy and Computers, *Privacy and Computers* (Ottawa: Information Canada, 1972) [hereinafter "Task Force, *Privacy*"].

[12] *Id.*, "Introduction".

[13] *Id.*, at 16.

[14] See *R. v. Plant*, [1993] S.C.J. No. 97, [1993] 3 S.C.R. 281 (S.C.C.) and *R. v. M. (A.)*, [2008] S.C.J. No. 19, 2008 SCC 19 (S.C.C.).

[15] For a good discussion of the problem of "bits" in the context of the dog-sniffer cases, see Ian Kerr & Jena McGill, "Emanations, Snoop Dogs and Reasonable Expectations of Privacy" (2007) 52:3 Crim. L.Q. 392.

Supreme Court of Canada decision *Spencer* calls this distinction between bits and systems into question, although it does not get rid of it entirely. In recognizing a reasonable expectation of privacy in subscriber information, and also in recognizing that informational privacy protects an interest in anonymity, *Spencer* brings the Charter understanding of privacy and the *Privacy Act* understanding of privacy closer together.

In *Spencer*, the Supreme Court held that the police must get a warrant to obtain subscriber information from telecommunications companies, and that informational privacy contemplates the protection of anonymity. One of the challenges in the case was to understand whether subscriber information attracted a reasonable expectation of privacy. The Supreme Court acknowledged that sometimes it is difficult to determine the "subject matter of the search" and that when it is difficult then the Court "has taken a broad and functional approach to the question, examining the connection between the police investigative technique and the privacy interest at stake".[16] Therefore instead of considering whether subscriber information understood as some kind of isolated bit of data attracts a reasonable expectation of privacy (or is merely like phone book information, an analogy pressed by the Crown), we need to understand that the police were seeking subscriber information in order to identify a particular individual and link him to his online activities. In doing so, police infringed that individual's anonymity. This shift from asking about the privacy interest in the "bit" of information to situating collection of the "bit" within a technique takes us towards thinking about privacy in information systems.

Another important aspect of *Spencer*'s discussion of anonymity is the Court's acknowledgment of privacy in public. *Spencer* follows the trajectory of *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*[17] in acknowledging that individuals can have privacy interests in information exposed to the public in some way. According to the Court, "[t]he mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a person may not be able to control who observes him or her in public."[18] Anonymity is engaged

---

16 *Spencer*, *supra*, note 7, at para. 26.

17 [2013] S.C.J. No. 62, [2013] 3 S.C.R. 733, 2013 SCC 62 (S.C.C.).

18 *Spencer*, *supra*, note 7, at para. 44.

where activities are in "public" but the author's identity in relation to those activities is not public.

This is important because it responds to some of the same concerns that animate data protection law and underpin its safeguards regarding dissemination. The idea is that an individual might be willing to share information with one person but not want that information shared with some other party. One of the core ideas of data protection law is that personal information can only be used or disclosed for the purposes for which it was collected, unless the individual consents. There are, of course, exceptions that reflect the need to balance privacy against other interests. However, this basic idea is what has also informed Charter jurisprudence regarding the continuing reasonable expectation of privacy an individual might have in information that has been shared with the state.[19] The fact that the state has collected information, voluntarily or not, does not void a reasonable expectation of privacy in relation to uses of that information that go beyond that original collection. The recognition of privacy in public is simply an extension of this principle, but a very welcome one. What it recognizes is that there is no crude public/private dichotomy but rather multiple social spheres in which we live; just because people in one sphere of life know things about an individual does not mean that others in another sphere of life must know the same things. This is a crucial insight for understanding the privacy implications of information systems, for the technological and operational impetus behind these systems is to aggregate and match data. In doing so, systems easily take information collected in one context and make it available for use in another context, raising privacy concerns.[20] By putting together the insight that privacy is not all-or-nothing with the insight that one can focus on techniques and not just "bits", there is an emerging basis to build upon for constitutionally assessing information systems.

If we read *Spencer* as attentive to techniques rather than "bits" then I think we also avoid a potential misinterpretation of the case. It is not accurate to say that *Spencer* moves away from a biographical core analysis to embrace personally identifying information, such as subscriber

---

[19] See, *e.g.*, *R. v. Mills*, [1999] S.C.J. No. 68, [1999] 3 S.C.R. 668 (S.C.C.). One could argue that this already shows the migration of data protection law ideas to constitutional law but a discussion of this migration is beyond the scope of this article.

[20] Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public" (1998) 17 Law & Philosophy 559; Lisa M. Austin, "Privacy and the Question of Technology" (2003) 22 Law & Philosophy 119 [hereinafter "Austin, 'Privacy'"].

information, as attracting Charter protection. There are a number of aspects of the decision that cut the other way. For example, the Supreme Court was not concerned about identification *per se* but emphasized that the police were trying to link a particular person to specific and monitored online activities that were engaged in anonymously; it is this context of identification that is important. The Supreme Court also sometimes uses the language of "intimate or sensitive activities being carried out online", which suggests a narrow scope for the protection of anonymity — the ability to engage in publicly visible activities that are sensitive and intimate.[21] This suggests that there remains a "privacy" threshold for Charter scrutiny, but the privacy interest must be assessed in light of the investigatory *technique* rather than simply by looking at the nature of the information in isolation.

One aspect of recent jurisprudence that cuts the other way can be seen in Moldaver J.'s reasons in *Wakeling*. In discussing whether the sharing of lawfully obtained wiretap information with a foreign state attracts section 8 scrutiny, Moldaver J. stated that the "disclosure of previously intercepted communications" is not a search.[22] However, he held that section 8 nonetheless did apply, since "[t]he highly intrusive nature of electronic surveillance and the statutory limits on the disclosure of its fruits suggest a heightened reasonable expectation of privacy" that is not extinguished once the communications are held by law enforcement agencies.[23] This suggests that apart from the special case of wiretaps, Moldaver J. would equate a "search" under the Charter with the *collection* of information rather than with its subsequent use or disclosure. If this is true, then the ability of section 8 jurisprudence to deal with information techniques and systems, rather than "bits", will be seriously compromised. Justice Moldaver's approach also lies in tension with the basic test for a search or seizure, which is simply whether a reasonable expectation of privacy has been intruded upon. The general reasonable expectation of privacy test is consistent with the mandate to interpret the Charter in a broad and purposive manner, rather than Moldaver J.'s "plain meaning" interpretation of the word "search".[24] However, Moldaver J. (with LeBel and Rothstein JJ.) was not in the majority with his approach. For McLachlin C.J.C., section 8 can protect against unreasonable uses of

21 *Spencer*, *supra*, note 7, at para. 66.
22 *Wakeling*, *supra*, note 8, at para. 32.
23 *Id.*, at para. 39.
24 *Id.*, at para. 34.

lawfully obtained information.[25] For Karakatsanis J. (with Abella and Cromwell JJ.), the question was only whether there was a residual reasonable expectation of privacy in the information.

III. The Lingering Question About Bits

One of the lingering questions regarding *Spencer* is how to understand the claim that requiring a warrant for subscriber information does not impact upon other types of more routine investigations where police officers might request information from third parties. The Supreme Court discussed this issue and Cromwell J.'s comments are worth quoting in full:

> The intervener the Attorney General of Alberta raised a concern that if the police were not permitted to request disclosure of subscriber information, then other routine inquiries that might reveal sensitive information about a suspect would also be prohibited, and this would unduly impede the investigation of crimes. For example, when the police interview the victim of a crime, core biographical details of a suspect's lifestyle might be revealed. I do not agree that this result follows from the principles set out in these reasons. Where a police officer requests disclosure of information relating to a suspect from a third party, whether there is a search depends on whether, in light of the totality of the circumstances, the suspect has a reasonable expectation of privacy in that information: *Plant*, at p. 293; *Gomboc*, at paras. 27-30, *per* Deschamps J. In *Duarte*, the Court distinguished between a person repeating a conversation with a suspect to the police and the police procuring an audio recording of the same conversation. The Court held that the danger is "not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words": at pp. 43-44. Similarly in this case, the police request that the ISP disclose the subscriber information was in effect a request to link Mr. Spencer with precise online activity that had been the subject of monitoring by the police and thus engaged a more significant privacy interest than a simple question posed by the police in the course of an investigation.[26]

The Court clearly views the request for subscriber information differently from "other routine inquiries" but the basis for this is not

---

[25] *Id.*, at para. 95.

[26] *Spencer*, *supra*, note 7, at para. 67.

entirely clear. Justice Cromwell suggests that there is a "more significant privacy interest" at issue here because the police were trying to identify the individual associated with specific activities. But that cannot be the entire basis of the distinction, for it suggests that the police would need a warrant whenever they ask questions of third parties that are aimed at identifying the perpetrator of a specific crime, or have a high likelihood of such identification.

Justice Cromwell, in adverting to *Duarte*, also invokes the issue of technology affecting the nature of the privacy interest. There are many debates in privacy that go something like the argument that was put to the court in *Duarte*: if I can tell the police what you told me then why is it any different for me to record this and pass along the recording? And if I can pass along the recording, why is it any different for the police to just record our conversation directly? The Supreme Court has called the latter a "much more insidious danger", but the basis of this remains unclear as we can see from the argument in *Spencer* — why is the voluntary provision of subscriber information more problematic than the voluntary provision of other identifying information in more "routine" forms of investigation?

Sometimes people point to "practical obscurity" as a way of understanding the difference that technology makes to our expectations of privacy.[27] For example, public records that are in paper format and stored in specific physical locations are very different from public records that are compiled centrally, electronically or otherwise. The distributed paper records are difficult to find and compile, so that the people they concern are protected by a kind of practical obscurity. Technology, in removing those practical barriers to access and compilation, eradicates the practical obscurity. In this way, the practical protection of privacy is altered even if in both cases (paper access and electronic access) the records are, in a normative sense, publicly available. There is something like this concern in the context of access to subscriber information. Many privacy advocates were worried that the absence of a warrant requirement to access subscriber information would lead to a situation where this was routinely asked for and provided, enabling other types of investigative techniques. Indeed, there is evidence that this was exactly what was happening prior to the *Spencer*

[27] See Austin, "Privacy", *supra*, note 20.

decision.[28] Warrantless access to subscriber information on a large scale effectively brings an end to anonymity on the Internet.

I have argued elsewhere that we should also think in terms of "practical constraint" as a way of understanding the difference that technology makes.[29] Constitutional jurisprudence regarding privacy is not simply about defining the nature of the privacy interest at stake but is also about ensuring basic rule of law values concerning constraints on public power. The worry in cases like *Duarte* is about the systemic effects of permitting the state, in its sole discretion, to determine whether and when to record conversations. The key issue here is the "unfettered discretion" of the state and what it means in the context of a particular technology. Sometimes technology removes a number of "practical constraints" that serve to fetter the discretion of the state even if it is not always obvious. A simple example is when technology brings down the cost of some types of investigatory techniques. If they are costly to engage in then the state has a reason to ensure that they are used carefully and only when necessary; once such techniques become easy and cheap then these practical constraints on their use are removed.

The practical constraint argument about the voluntary provision of subscriber information from telecommunications companies is this. When investigatory methods rely upon the participation of community members the police have to ensure that they maintain the trust of the community or else there will be no participation. Community members exercise their own judgment regarding whether and when to cooperate with police and this can be informed by many things, including the perceived legitimacy of the police investigation. Even where the community is not asked to cooperate but police actions are public and visible, potential community reaction to their methods is a practical constraint on what they might choose to do. Investigations that rely on community involvement can also be resource intensive. All of these things change when the police ask for access to data from intermediaries such as telecommunications companies — it is relatively cheap, invisible

---

[28] Alex Boutilier, "Millions of police requests for Canadians' data every year, documents show", *The Toronto Star***,** July 21, 2014, online: <http://www.thestar.com/news/canada/2014/07/21/millions_of_police_requests_for_canadians_data_every_year_documents_show.html>.

[29] Lisa M. Austin, "Enough About Me: Why Privacy is About Power, Not Consent (or Harm)" in Austin Sarat, ed., *A World Without Privacy?: What Can/Should Law Do* (NY: Cambridge University Press, 2014).

to the public and the intermediaries exercise their judgment to cooperate in a context far removed from the community of the people affected.

The difference, therefore, between subscriber information and other information that might be requested by the police does not lie in the nature of the information itself. It has to be understood in relation to the investigatory techniques and systems that form the context for its collection and use, and how this enables a change in both privacy and accountability, understood in terms of both practical obscurity and practical constraints.

IV. Safeguards and the Life Cycle of Information

In several recent Supreme Court cases, notably *Wakeling* and *Fearon*, the issue of "safeguards" was prominent in the analysis of reasonableness under section 8. This is interesting, for a number of the concerns raised are of the type at home in data protection law such as concerns about safeguards to limit subsequent uses of information by third parties. This suggests another way in which section 8 jurisprudence is moving towards a framework that will allow it to deal with the privacy implications of information systems by considering the life cycle of the information collected. Just like a focus on "bits" of information obscures the role of investigative techniques, a focus on a particular moment of collection or disclosure obscures the broader life cycle of information and the types of vulnerabilities associated with aspects of this cycle.

Wakeling concerned the constitutionality of *Criminal Code*[30] provisions that permit the disclosure of lawfully obtained wiretap information with foreign authorities. The Supreme Court split three ways. Justice Moldaver (with LeBel and Rothstein JJ.) held that while there are residual privacy interests associated with wiretap information once obtained by the state, the legislative framework for information sharing in the *Criminal Code* is reasonable. Justice Karakatsanis (with Abella and Cromwell JJ.) also held that lawfully obtained wiretap information still retained a reasonable expectation of privacy but found the legislative framework for disclosure unreasonable. Chief Justice McLachlin held that although there can be an expectation of privacy in information held by the state, section 8 is not engaged where the information was collected for law enforcement purposes and is shared for law enforcement purposes.

---

[30] R.S.C. 1985, c. C-46.

The major dispute between Moldaver and Karakatsanis JJ. was over the issue of safeguards, not privacy *per se*. Privacy violations are constitutionally acceptable if authorized by a reasonable law and carried out in a reasonable manner. This question of "reasonableness" was the grounds of the disagreement and the dispute turned on whether safeguards are constitutionally *required* in order for the privacy violation contemplated by the sharing to be found reasonable for the purposes of section 8. According to Karakatsanis J., "[t]o render the scheme constitutional, Parliament must require the disclosing party to impose conditions on how foreign officials can use the information they receive, and must implement accountability measures to deter inappropriate disclosure and permit oversight."[31] In contrast, Moldaver J. declined to require these safeguards in order to render the statute reasonable but did indicate that in some factual contexts safeguards might be required in order for the actual disclosure to be carried on in a reasonable manner. Some of the types of safeguards mentioned in the decision include information-sharing protocols, caveats, record-keeping and reporting or notice obligations.

The other recent case to discuss the issue of safeguards is *Fearon*. *Fearon* concerned the constitutional permissibility of a warrantless search of a cell phone incident to lawful arrest. Justice Cromwell, for the majority, held that such searches do not violate section 8 of the Charter. However, he also held that the common law framework for searches incident to arrest required modification for cell phone searches in order to add extra safeguards to protect privacy. In addition to requiring the arrest to be lawful and the search truly incidental to the arrest, Cromwell J. required a strict tailoring of the search that would limit what could be accessed and also that the police make records about what they accessed and how.[32] Record keeping points to another dimension of safeguards, which is the possibility of after-the-fact review. Searches of phones and computers are not "public" in the sense that those affected can know what was searched and potentially complain about overreach or abuse. Record-keeping requirements permit a form of review regarding whether the police stayed within the boundaries of their authorization.

---

[31] *Wakeling*, *supra*, note 8, at para. 105.

[32] Justice Cromwell also endorsed the use of notes in computer searches in *R. v. Vu*, [2013] S.C.J. No. 60, [2013] 3 S.C.R. 657, 2013 SCC 60, at para. 70 (S.C.C.).

If the idea of safeguards is developed within Charter jurisprudence, a lot could potentially be learned from the data protection law framework since so much of it concerns ensuring the information is only used for the purposes it was collected. This raises many additional questions, not dealt with here, concerning how to operationalize these insights for the institutional structure and institutional competencies of the Canadian data commissioners is quite different from that of the courts and justices of the peace who traditionally oversee warrants. Even if much is to be gained *normatively* from these frameworks informing one another, these other important practical issues remain.

V. Different Protective Frameworks and the Question of Balance

There remain significant differences between the constitutional framework and the data protection law framework when it comes to two sets of ideas: (1) necessity and proportionality and (2) accountability. By necessity and proportionality I mean the basic idea that intrusions into an individual's privacy interest must be justified. Most justification tests incorporate both the idea that the intrusion is necessary, limited to only that which is necessary, and that the benefit is proportional to the losses associated with the intrusion. By accountability I mean the various legal mechanisms that ensure that the only privacy invasions permitted are those that are necessary and proportional, including both prior authorizations and after-the-fact review.

The data protection regime was developed to address the information practices of the administrative state, especially in the context of the increasing combination of computer technology and bureaucratic information systems. Its paradigm case is the collection of personal information in order to provide some kind of government benefit or service to an individual. The ideas of necessity and proportionality operate here to ensure, in a variety of ways, that only personal information needed for the provision of that benefit or service is collected, and that this personal information is only used or disclosed in order to provide that benefit or service unless the individual consents. In this paradigm administrative case, the individual *wants* the benefit or service at issue. The individual interest is therefore not aligned with *prohibiting* the state from collecting, using or disclosing personal

information for the purposes of providing that benefit or service — the individual interest lies in ensuring there is no over-collection, no function creep and no inaccuracies. One of the key accountability mechanisms in such legislation is the right granted to individuals to access their own personal information in order to see what has been collected and to ensure its accuracy. There are many contexts that depart from this paradigm case, and many criticisms that could be made regarding whether particular legislation, like the *Privacy Act*, properly ensures such necessity and proportionality.[33] However, this basic picture can help to highlight the differences between this and the constitutional context, which is primarily concerned with law enforcement. Indeed, the *Privacy Act* offers very weak protection in the context of law enforcement and national security because of the number of exceptions to the usual operation of the Act that are engaged in such contexts.

Another way to understand the kind of protection offered by data protection law is to see it as an example of what it means to bring state information practices within a regime of law. As the Task Force on Privacy and Computers reported so many years ago, computerized information systems can concentrate power in the hands of those who operate them.[34] In liberal democracies, it is the ideal of the rule of law that addresses our concerns about power. According to Waldron, "the Rule of Law aims to correct abuses of power by insisting on a particular mode of the exercise of political power: governance through law."[35] Postema echoes this point, arguing that throughout its history the rule of law "has been rooted in the two-fold thought that a polity is well-ordered when its members are secured against the arbitrary exercise of power and that law, because of its distinctive features, is especially if not uniquely capable of providing such security".[36] The rule of law is traditionally thought to encompass two different ideas: that law should provide guidance to individuals and that law should constrain public power. In many ways, data protection law aims to ensure that government information practices are consistent with these very basic

---

[33] Indeed, the *Privacy Act* is much weaker in this respect than the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [hereinafter "PIPEDA"], which applies to the private sector.

[34] Task Force, *Privacy*, *supra*, note 11, at 18.

[35] Jeremy Waldron, "The Concept and the Rule of Law" (2008) 43 Georgia L. Rev. 1, at 11.

[36] Gerald J. Postema, "Fidelity in Law's Commonwealth" in Lisa M. Austin & Dennis Klimchuk, eds., *Private Law and the Rule of Law* (Oxford: Oxford University Press, 2014).

ideas of the rule of law. Guidance is accomplished through the idea that individuals should know what information the government is collecting about them and how it will be used. Constraints on power are accomplished through measures that ensure that information is only collected and used in these ways, and that exceptions are clearly outlined in public laws.

The constitutional regime of privacy, in contrast, was developed in the law enforcement context where the focus is on unreasonable search and seizure. Here the individual interest lies very much in *prohibiting* state collection of information, not in facilitating its access for specific purposes. That is because, of course, the law enforcement purpose is what brings the individual into a conflictual relationship with the coercive role of the state. The paradigm case is one where the state seeks a warrant in order to get permission to do something it cannot otherwise do — instead of seeking to make its information practices generally lawful it is seeking a specific *exemption* from the law. In order to pursue the general rule of law goal of upholding the law, state agents sometimes require authorization to do what is otherwise impermissible. This is justified only to the extent necessary to uphold the law more generally. The basic standard, endorsed in *Hunter v. Southam*,[37] and expressed in the *Criminal Code*, is that the state must show reasonable grounds to believe that a crime has been committed and that the search will yield evidence (the reasonable and probable grounds standard). Accountability measures cannot be ones that rely upon the individual, but instead involve an objective party like a judge who determines whether the threshold has been met through a process of prior authorization (for example, through issuing a warrant).

One context where it is important to keep in mind these differences between the two frameworks is when the data protection law framework is invoked as an appropriate model of privacy protection in the context of law enforcement or national security. For example, one of the elements proposed by President Obama for strengthening the privacy rights of non-U.S. persons in relation to U.S. surveillance practices is to extend the protections of the U.S. *Privacy Act* to non-U.S. persons (but not the U.S. Fourth Amendment).[38] Another example is the "Statement of

---

[37] [1984] S.C.J. No. 36, [1984] 2 S.C.R. 145 (S.C.C.) [hereinafter "*Hunter*"].

[38] Office of the Press Secretary, "Presidential Policy Directive/PPD-28", *The White House*, January 17, 2014, online: The White House <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

Privacy Principles by the United States and Canada" associated with the Canada-U.S. Beyond the Border Plan, a plan that seeks greater information sharing between the two countries for the purposes of border security.[39] These principles reflect the Fair Information Practices of data protection law, not constitutional law.[40] And more recently still, the Canadian government's defence of its new anti-terrorism legislation and its robust inter-governmental information sharing provisions, relied heavily upon the proposition that privacy is protected through the application of the federal *Privacy Act*.[41] Given the fact that the paradigm for data protection law is not the coercive state-individual relationship contemplated by search and seizure law, and given that there are so many exceptions for law enforcement and national security in the data protection law context, we should be very wary of this pattern of enlisting the data protection law model in this way.

There is some thought that injecting a strong test for necessity and proportionality into the data protection law framework can help shore up its potential defects.[42] As outlined in the introduction, the Office of the Privacy Commissioner of Canada has proposed this as a part of the Privacy Impact Assessment process under the *Privacy Act*, and sees this very much as importing a kind of constitutional test for justification for limits to privacy. However, the constitutional test that the Privacy Commissioner invokes is the *Oakes* test that governs the interpretation of section 1 of the Canadian Charter — which is the general provision that allows for limits on constitutional rights and freedoms if they can be demonstrably justified in a free and democratic society. What the Privacy Commissioner's approach does not grapple with is the fact that section 8 of the Charter, which protects a reasonable expectation of privacy, also involves balancing and justification and some of the considerations that are appropriate within section 8 are ones that bear consideration when seeking to "constitutionalize" data protection law when the latter is enlisted in the law enforcement and national security context.

---

[39] See Beyond the Border Action Plan, "Statement of Privacy Principles by the United States and Canada", Public Safety Canada, May 30, 2012, online: <http://actionplan.gc.ca/en/backgrounder/bap-paf/statement-privacy-principles-united-states-and-canada>.

[40] It might be that, prior to *Wakeling*, the government did not think that cross-border information sharing attracted Charter scrutiny.

[41] See Austin, "Anti-Terrorism's Privacy", *supra*, note 4.

[42] The federal private sector privacy legislation, PIPEDA, achieves a version of this with its reasonable purposes test in s. 5(3), which has been interpreted in a manner that follows the *Oakes* test very closely.

It is worth emphasizing how the idea of justification that yields the reasonable and probable grounds standard in section 8 works differently than the section 1 analysis under the Charter. Both incorporate the basic ideas of necessity and proportionality that underpin any justificatory test. However, of the three parts of the *Oakes* test — rational connection, minimal impairment and the proportionality of deleterious effects — it is minimal impairment that is the real workhorse. Although there have been a few cases that have discussed the importance of the third prong of the test, it rarely does any real work.[43] The situation is different with the "balancing" internal to the section 8 analysis. "Balancing" always has a very feeble sound to it, but there is nothing feeble about the reasonable and probable grounds standard. Here, it is not the idea of minimal impairment that does all the work. The reasonable and probable grounds standard is *not* about how to permit the state to pursue its law enforcement objective while impairing privacy as minimally as possible. Instead, it incorporates ideas that are more about the proportionality of deleterious effects.

Such a high standard means that sometimes the law enforcement goal will *not* be met. Indeed, this is contemplated by the section 8 balancing itself. As Dickson J. states in *Hunter*, the very question is when the individual's expectation of privacy "must give way to the government's interest in intruding on the individual's privacy in order to advance its goals".[44] The idea is *not* that privacy must give way so long as it is intruded upon as minimally as possible but that law enforcement goals hold sway only at a particular point marked by the probable effectiveness of reaching that goal. This focus on the likely *effectiveness* of the state action reaching its goal is missing in the standard section 1 analysis, in part because that test has been developed in the context of reviewing social legislation.[45] As the Supreme Court cautioned in *Hutterian*, "a government enacting social legislation is not required to show that the law will in fact produce the forecast benefits. Legislatures can only be asked to impose measures that reason and the

---

[43] See *Canada (Attorney General) v. JTI-Macdonald Corp.*, [2007] S.C.J. No. 30, [2007] 2 S.C.R. 610 (S.C.C.), *Alberta v. Hutterian Brethren of Wilson Colony*, [2009] S.C.J. No. 37, [2009] 2 S.C.R. 567 (S.C.C.) [hereinafter "*Hutterian*"] and *New Brunswick (Minister of Health and Community Services) v. G. (J.)*, [1999] S.C.J. No. 47, [1999] 3 S.C.R. 46 (S.C.C.).

[44] *Hunter*, *supra*, note 37, at 159-60.

[45] I would like to thank Julia Dryer for this insight.

evidence suggest will be beneficial. If legislation designed to further the public good were required to await proof positive that the benefits would in fact be realized, few laws would be passed and the public interest would suffer."[46] However, when the state is using its coercive power to act against an individual's interests in a manner that is usually not permitted, then this issue of effectiveness, and proportionality, is of crucial importance.

VI. MERGING FRAMEWORKS?

If the Charter is going to deal with "Big Data" techniques, then Charter privacy jurisprudence needs to continue to move away from thinking about "bits" of information and towards thinking about systems of information. It also has to move away from thinking about discrete informational transactions and think more about the entire process of collection, use and disclosure within such systems so that adequate safeguards are required. As I have outlined, there are promising signs that the jurisprudence is moving in this direction. In doing so, the constitutional framework can learn from the data protection law framework. At the same time, if the data protection law framework is going to provide meaningful privacy protection in the context of Big Data techniques for law enforcement and national security purposes, then the fact that it has not been developed in the context of the coercive state-individual relationship at issue in law enforcement and national security must be confronted. Developing tests for the "necessity and proportionality" of information practices, for example, that do not properly attend to the legal contexts in which the tests have been developed are unlikely to provide robust privacy protection. Nonetheless, something like a merger of the two frameworks is what is required to deal with the emerging world of Big Data as it applies within law enforcement and national security investigations. This article concludes with offering a sketch of a model of what such a merger might look like.

Consider the Snowden revelations concerning the use of airport Wi-Fi data in a trial run of a new software program being developed by CSE for use in tracking targets. The revealed slides show how the bulk collection of the data of people who are not under suspicion at all can be

[46] *Hutterian*, *supra*, note 43, at para. 85.

used to track and locate an individual who is under investigation — in the technique tested it could "be used for any target that makes occasional forays into other cities/regions".[47] *Spencer* would suggest that when the technique is used to find a particular network ID of interest then matching that ID with other personally identifying information would trigger section 8. The Big Data question has to do with what happens prior to the identifying moment, when data about a large number of people — such as a "sweep" of an entire city — is collected in order to find the ID of interest. Many of the new metadata production orders and warrants enacted by the recent lawful access provisions in Bill C-13 allow such information (transmission data and tracking data) to be collected on the standard of "reasonable suspicion" that the information "will assist in the investigation of the offence".[48] This is a very low standard and looks like it is meant to enable the collection and analysis of the "haystack".

One response is to argue that transmission and tracking data, like other forms of metadata, can have the same privacy implications as the subscriber information at issue in *Spencer*, and can be more revealing than the contents of communications. If so, it should be protected by the higher standard of the general production order in the *Criminal Code*, which is "reasonable grounds to believe … will afford evidence respecting the commission of the offence".[49] In other words, access to this information should conform to the same standards we apply regarding access to the content of communications.

Another response is to move away from a focus on the "bits" of information and focus instead on the information systems, or techniques, they are a part of. The issue with metadata is that it is sometimes highly revealing and sometimes not, depending on how it is used. Our constitutional tests need to capture this "it all depends" quality. Because "it all depends" there are also concerns about its misuse — it might be used in a manner that is considered minimally privacy-invasive but

---

[47] The CBC posted the slides online: <http://www.cbc.ca/news2/pdf/airports_redacted.pdf>. See also Greg Weston, Glenn Greenwald & Ryan Gallagher, "CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents", CBC News, January 30, 2014, online: <http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>.

[48] See, for example, s. 487.016 of the *Criminal Code*.

[49] Section 487.014(2).

stored insecurely and open to misuse, for example. So this information brings along with it a strong concern regarding safeguards.

One way to get at this would be to think about Big Data techniques in three parts. The first would be the development of the technique itself. As we can see from the Snowden revelations, these techniques are developed and tested for their effectiveness. They should also be subject to independent review for their privacy impact, where both privacy law experts and technical experts could determine whether the techniques could be made more privacy-protective in any way. This would be a kind of minimal-impairment analysis and the issue of safeguards would be prominent. The second part of the analysis would be judicial oversight of the use of the technique. Instead of focusing on permission to collect the "bits" of hay in the haystack, the permission sought would be for the needle-in-a-haystack technique as a whole. There is no reason why this cannot be with the standard warrant or production order process already in the *Criminal Code* — in order to deploy the technique the state would have to show that it has reasonable grounds to believe an offence has been or will be committed and the use of the technique will afford evidence of the offence. If this is authorized, then the information collection and use contemplated by the technique — and already independently reviewed in the first step — is also authorized. The third part of the analysis would be to provide for after-the-fact review. Because one of the main privacy concerns regarding the use of such techniques is their effect on innocent third parties whose information is collected and used, another level of after-the-fact review is important to assess the overall effectiveness of such techniques and how this is balanced against their overall impact on privacy.

There are three "moments" then, to this proposal. First, an independent privacy impact assessment when developing an investigatory technique. Second, judicial oversight in relation to when such techniques can be deployed, using the usual standards rather than relaxed standards. Third, independent and systemic after-the-fact review aimed at understanding whether the overall effectiveness of such techniques is proportional to the overall impact on privacy. The proposal makes use of aspects of both the constitutional framework for privacy protection and the data protection law framework.

Increasingly, we will need to find ways to merge the two frameworks in order to provide a public law of privacy adequate to the information age. This article has tried to offer some initial thoughts on why this is important and how it might work, drawing upon recent jurisprudence and recent events. What we need is a broader and more sustained critical conversation about the public law of privacy in order to meet these emerging challenges.