Washington University Global Studies Law Review

Volume 16 | Issue 3

2017

Section Eight, Pipeda, and the Problem of Shifting Norms: A Case for a Contract Model of Data Privacy

John D. Perry
Staff Editor, Washington University Global Studies Law Review; J.D. (2017), Washington University School of Law; A.B. (2012), Princeton University

SECTION EIGHT, PIPEDA, AND THE PROBLEM OF SHIFTING NORMS: A CASE FOR A CONTRACT MODEL OF DATA PRIVACY

INTRODUCTION

In recent years, governmental and private entities have engaged in unprecedented data-collection practices.[1] Edward Snowden's 2013 leak regarding the NSA's bulk telephony metadata program was only the "tip of the iceberg" when viewed alongside the burgeoning private marketplace for personal data.[2] Today, "Big Data" firms comprise a multi-billion-dollar industry in which personal information is "bartered and sold" to the highest bidder.[3] Low access-costs of social media sites, blogs, and other forms of internet media ensure a constant flow of personal information that firms collect and analyze to create "full-scale psychological profile[s]" of consumers.[4] According to the International Data Corporation, the "global volume of data" will double every two years and, at its current trajectory, will balloon to over "40 trillion gigabytes" by 2020.[5]

---

1. *See* Jason M. Weinstein, William L. Drake & Nicholas P. Silverman, *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era,* 52 AM. CRIM. L. REV. 729, 732 (2015); Lee Raine & Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RESEARCH CENTER (Feb. 19, 2016), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns.

2. Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. NAT'L SECURITY L. & POL'Y 333, 339 (2014); Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 64-67 (2000).

3. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1407 (2001); *see* Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U.L. REV. 859, 867-69 (2016) ("Given the novelty of Big Data-informed analytics, the public is largely unaware of the rapid growth of the data industry and the extent to which individuals' personal information has become a commodity that is transferred among private and public entities"); EXECUTIVE OFF. OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014) (at 50, "[Private information] is bought, bartered, traded, and sold. An entire industry now exists to commoditize the conclusions drawn from that data.");

> At the broadest level, we are building an Internet that is on its face free to use, but is in reality funded by billions of transactions where advertisements are individually targeted at Internet users based upon detailed profiles of their reading and consumer habits. Such "behavioral advertising" is a multibillion-dollar business, and is the foundation on which the successes of companies like Google and Facebook have been built.

Neil M. Richards, *The Dangers of Surveillance,* 126 HARV. L. REV. 1934, 1938 (2013) (internal citations omitted).

4. Solove, *supra* note 3, at 1404; *see* Jacques Bughin, Michael Chui, and James Manyika, *Clouds, Big Data, and Smart Assets: Ten Tech-Enabled Business Trends to Watch*, McKinsey Quarterly 7-8 (2010), available at http://www.itglobal-services.de/files/100810_McK_Clouds_big_data_and% 20sm-art%20assets.pdf.

5. IDC Big Data and Business Analytics Forum 2013: Leveraging Data for Agile Business, INT'L DATA CORP. (Nov. 26, 2013), http://idc-cema.com/eng/events/50534-idc-big-data-and-business-analytics-forum-2013.

Canada has struggled to adapt its privacy law to the Big Data paradigm. While the Personal Information Protection and Electronic Documents Act ("PIPEDA")[6] has enhanced data security among users and service providers, the act has done little to restrict or establish coherent parameters for information sharing among service providers and law enforcement agencies.[7] Judicial enforcement of Section Eight of the Charter of Canadian Rights and Freedoms ("Section Eight"),[8] moreover, has had limited effect in carving out expectations of privacy independent of existing legislative and regulatory frameworks.[9] Without this independence, the courts neglect their duty under Section Eight to judicially review statutes that intrude on reasonable expectations of privacy.[10]

The difficulty Canadian lawmakers and courts face when crafting data privacy protections stems not so much from identifying minimal privacy standards as it does from wide variations in data privacy norms.[11] Social media users, for example, vary significantly in the types of information they are willing to share online.[12] For those who broadcast personal (perhaps incriminating) details about their lives to large groups of individuals online, society's need to prosecute crime probably outweighs the need to recognize those individuals' privacy interests.[13] But the calculus

---

6. Personal Information Protection and Electronic Documents Act (hereinafter referred to as "PIPEDA"), S.C. 2000, c. 5 (Can.).

7. *See* Graham Mayeda, *Privacy in the Age of the Internet: Lawful Access Provisions and Access to ISP and OSP Subscriber Information*, 53 ALTA. L. REV. 709, 714-15 (2016); Matthew Nied, *Cloud Computing, the Internet, and the Charter Right to Privacy: The Effect of Terms of Service Agreements on Reasonable Expectations of Privacy*, 69 ADVOC. VANCOUVER 701, 702-05 (2011); Daphne Gilbert, Ian R. Kerr, and Jena McGill, *The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers*, 51 CRIM. L. Q. 469, 472 (2007).

8. Canadian Charter of Rights and Freedoms, s 8, Part I of Constitution Act, 1982, being Schedule B to the Canada Act 1982, c 11 (U.K.). (hereinafter referred to as "*Section Eight*").

9. *See generally* R v. Spencer, [2014] 2 S.C.R. 212, paras. 53-67 (Can.); R. v. Gomboc, [2010] 3 S.C.R. 211, para.31 (Can.); R. v. Mahmood, 2008 CanLII 51774, para. 56 (ON SC).

10. Mayeda, *supra* note 7, at 46-48.

11. Many commentators have noted a "privacy paradox," or the discontinuity between people's general desire for privacy, on the one hand, and their seemingly incongruous willingness to share private information. *See* H. Brian Holland, *Privacy Paradox 2.0*, 19 WIDENER L.J. 893, 893-94 (2010). The paradox demonstrates that at least for some people the convenience and adaptability of online communications (e.g. social media, email, blogging, etc.) might outweigh the value of increased privacy protections. *See* Stephanos Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 597, 603-04 (1994); DANIEL J. SOLOVE, *UNDERSTANDING PRIVACY* 41 (2008) ("Privacy is a product of norms, activities, and legal protections, and as a result, it is culturally and historically contingent.").

12. Patricia Sánchez Abril, *Private Ordering: A Contractual Approach to Online Personal Privacy*, 45 WAKE FOREST L. REV. 689, 698 (2010) ("Some social media participants covetously guard their privacy; the more conspicuous display an urge to divulge everything about themselves") (internal quotations omitted); *see* Solove, *supra* note 11 at 41.

13. *See* Richard Posner, THE ECONOMICS OF JUSTICE 233-239 (1981) (highlighting that greater privacy creates a social cost of insulating bad behavior and allows people to have more opportunities to manipulate each other); R. v. Laurin, 1997 CanLII 775m para. 41 (Can. ON CA) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *see generally* Brewer v.

becomes much less clear for individuals who use online technology to communicate with people they know and trust.[14] Even among those who share minimal personal information online, the trivial details they do share can become comprehensive biographies when aggregated by third-party service providers.[15] Law enforcement agents can then use these biographies to investigate and prosecute individuals for a wide-array of criminal conduct.[16]

The Supreme Court of Canada has begun to develop a promising jurisprudence based on a contractual right of privacy.[17] Faced with the prospect of adapting normative constraints to the increasingly more complex and wide-scale data collection practices, the court has begun to utilize privacy policies a user assents to as an indication of the user's reasonable privacy expectations.[18] Contract law, which potentially allows parties to negotiate constraints on privacy, is well-suited to handle

---

Williams, 430 U.S. 387, 416-17 (1977) (Burger, J. dissenting) (repudiating a "sporting theory of criminal justice," or one that views the Fourth Amendment as a substantive protection a defendant can assert to escape criminal liability).

14. In American jurisprudence, a person loses his or her privacy interest in information he or she shares with a third-party because, in sharing the information, the person has assumed the risk the information will be disclosed to law enforcement. United States v. Miller, 425 U.S. 435, 443 (1976) (holding that defendant did not have a reasonable expectation of privacy in his bank records); United States v. Graham, 824 F.3d 421, 427–28 (4th Cir. 2016) (holding that defendant did not have a reasonable expectation of privacy in historical cell-site location data since the defendant voluntarily disclosed his location data to cellular providers by using his phone); United States v. Meregildo, 883 F. Supp. 2d 523, 525-527 (S.D.N.Y. 2012) (finding that a Facebook user loses a privacy expectation with respect to information he or she shares to a Facebook friend). Canadian courts have largely rejected this doctrine. R. v. Cole, [2012] 3 S.C.R. 53, paras. 77-78 (Can.). Richard Epstein, moreover, offers a compelling critique of the doctrine. Richard Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L. J. 1199 (2009). Epstein argues that mere knowledge that one takes the risk that information can be exposed does not mean that one has assumed such risk. *Id.* at 1204. To reach the latter conclusion the individual would have to have some meaningful way to bargain about the risk he or she assumed. *Id.*; *see* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1872-74 (2016).

15. Solove, *supra* note 3, at 1404; Craig Forcese*, Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives*, *in* LAW, PRIVACY AND SURVEILLANCE IN CANADA IN THE POST-SNOWDEN ERA 127, 129-32 (Michael Geist ed., 2015); *see* Riley v. California, 134 S. Ct. 2473, 2491 (2014) (holding that, absent exigent circumstances, the government could not search a cell phone incident to a lawful arrest because, unlike more traditional items of property, a cell phone "contains a broad array of private information."); *see also* United States v. Jones, 132 S. Ct. 945, 956-57 (2012) (Sotomayor, J. concurring) (questioning the continued viability of the third-party doctrine in the digital age).

16. *See* Office of the Privacy Commissioner of Canada, *The Age of Predictive Analytics: From Patterns to Predictions* (2012), available at https://www.priv.gc.ca/media/1753/ pa_201208_e.pdf.

17. Cole, [2012] 3 S.C.R. 34, para. 52 (Can.); *see* cases cited *supra* note 9*;* R. v. Cuttell, 2009 ONCJ 471 (CanLII). Some American courts have suggested a similar principle. In United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010), for example, the Sixth Circuit stated that there may be circumstances in which a "subscriber agreement" is broad enough to defeat a reasonable expectation of privacy.

18. Cole, [2012] 3 S.C.R., para. 52; *see* cases cited *supra* note 9*;* Cuttell, *supra* note 17.

variations in the types of information people want to keep private.[19] So long as the law provides users opportunities to bargain over terms in their policies, a contract law framework can protect reasonable privacy expectations among users with diverse privacy preferences.[20]

This Note will proceed in two parts. In Part I, I will explain the current statutory and constitutional data privacy law in Canada. In Part II, I will set forth several recommendations about how courts and the legislature can create a framework in which terms of use and privacy policy terms can provide sufficient notice to users and allow them to have more meaningful bargaining power in negotiating privacy terms. Because Canadian and American search and seizure law both utilize the reasonable expectation of privacy test in determining whether a search or seizure is reasonable, this Note will often cite American cases that support similar principles in case and statutory law. However, the principal focus of this Note is Canadian privacy law.

PART I: EXISTING LEGAL PROTECTIONS FOR DATA PRIVACY

A. Personal Information Protection & Electronic Documents Act ("PIPEDA")

PIPEDA regulates the private sector's collection, use and disclosure of personal information in the course of commercial activities.[21] The Canadian Parliament passed PIPEDA primarily to ensure compliance with Article 25 of the European Union's Directive on Data Protection ("the Directive"),[22] which was necessary to preserve important trade relations with European Union (EU) members.[23] For this reason, the Directive can be viewed as a prototype of PIPEDA's core features. The Directive regulates data sharing among member and non-member states

19. *See* Abril, *supra* note 12, at 704; Bibas, *supra* note 11, at 597, 603-604.

20. *See* Abril, *supra* note 12, at 714-715.

21. R. v. Ward, (2012) 112 O.R. (3d) 321, para. 40 (Can. Ont. C.A.); *see* Tariq Ahmad, *Online Privacy Law: Canada,* LIBRARY OF CONGRESS, *https://www.loc.gov/law/help/online-privacy-law/canada.php*.

22. Council Directive 95/46, art.25, 1995 O.J. (L 281) 31 (EC) (hereinafter referred to as "The Directive."). Article 25(1) states in pertinent part:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

23. *See* Josh Nisker, *PIPEDA: A Constitutional Analysis*, 85 LA REVUE DU BARREAU CANADIEN 317, 318 (2006); Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357, 379 (2005).

and establishes an array of privacy principles for the collection of personal data.[24] These include rules on the processing of data, as well as requirements that service providers limit data collection to legitimate purposes,[25] obtain consent for personal data collection,[26] and allow users access to the data that service providers have collected.[27] Additionally, the Directive prohibits member EU states from sharing information with non-member countries whose data privacy laws do not provide users an "adequate level of protection."[28]

The Directive is significant in part for its limitations.[29] Since its primary focus is on the processing of information, the Directive's provisions relate to obligations imposed on data controllers and not to the protection of users' data ownership rights.[30] The Directive, moreover, allows member and complying non-member states to create a law enforcement exception to most of its data protections.[31] In crafting PIPEDA, the Canada national assembly incorporated the Directive's central provisions.[32] PIPEDA "recommends" that service providers explain the purpose for why they collect personal data, seek express consent when information is likely sensitive, develop a data retention policy, and account for third parties to whom they share information.[33] Like the Directive, PIPEDA also eschews recognition of a customer's ownership rights in his or her personal information, as service providers may collect, use, or disclose personal information according to an overarching reasonableness principle.[34] This reasonableness mandate, however, has not been interpreted as applying constraints on prospective uses of information. [35] PIPEDA, therefore, does not prohibit service

24. Nisker, *supra* note 23, at 318.
25. *See* The Directive, art. 7
26. *Id.*
27. *Id.* at art. 12-13
28. *Id.* at art. 25
29. *See* James R. Maxeiner, *Freedom of Information and the EU Data Protection Directive*, 48 FED. COMM. L. J.93, 97 (1995).
30. *Id.*
31. *Id.* at 103; The Directive, art. 13
32. Pursuant to Article 29 of the Directive, the EU Data Protection Working Party assessed whether PIPEDA ensured "adequate" data privacy protections. The Data Protection Working Party issued an opinion in 2001 that PIPEDA met the Directive standards. *See* Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electric Documents Act, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp39_en.pdf; s*ee* Mahmud Jamal, *Is PIPEDA Constitutional?*, 43 CAN.BUS.L. J. 434, 438-39 (2006).
33. PIPEDA, S.C. 2000, c.5, Sched.1, 4.2.3,5; 4.3.5,6; 4.5.2 (Can.).
34. PIPEDA, S.C. 2000, c.5, s.5(3) (Can.); Agathon Fric, *Access of Evil? Legislating Online Youth Privacy in the Information Age*, 12 CAN. J. L. & TECH. 141, 152 (2014).
35. *Turner v. Telus Communications Inc.,* [2007] F.C.A. 21, para. 15; *see* Fric, *supra* note 34, at 155.

providers from using novel technologies to generate more complete biographies of users based on data they previously disclosed.[36]

While the scope of PIPEDA's data protections is quite broad, it contains numerous collection, use and disclosure exceptions that constrain its privacy protections. First, PIPEDA's provisions are limited to commercial data collection.[37] In *McKesson v. Teamsters*,[38] the Ontario Arbitration court held that an employer who caught an employee's absence by "surreptitiously" making a video recording of him off-site did not violate PIPEDA because such monitoring was not made "in the course of commercial activities."[39] Second, while PIPEDA generally restricts service providers from collecting sensitive personal information from users, Section 7(1)(b) allows service providers to collect information without obtaining the subject's consent if they reasonably believe that: (1) obtaining consent would "compromise the availability…of the information" and (2) the information is of a type that could reasonably be expected to aid in investigating a "breach of an agreement or a contravention of the laws of Canada or a province." [40] Third, PIPEDA contains a contains a broad voluntary disclosure provision. Under Section 7(3)(c.1)(ii), a service provider may disclose personal information to a government agent who has "lawful authority" and who requests information: (1) relating to national security, (2) necessary for investigating and enforcing any breach of federal or provincial law, or (3) necessary to administer any federal or provincial law.

In *Spencer*, the Court had an opportunity to assess the meaning of "lawful authority" under 7(3)(c.1).[41] Rather than interpreting the provision as enhancing law enforcement's investigatory capabilities, the Court held that the provision merely codified the police's traditional, investigatory powers, including the authority of police to conduct a search in exigent circumstances.[42] The scope of PIPEDA's disclosure provisions, however, remains unclear in the wake of *Spencer*. Unlike the United States' Stored Communications Act (SCA), PIPEDA does not

36. *See* Fric, *supra* note 34, at 157.

37. PIPEDA, S.C. 2000, c.5, 4(1)(a); Chris D.L. Hunt, *The Common Law's Hodgepodge Protection of Privacy*, 66 U.N.B.L.J. 161, 181 (2015).

38. *McKesson Canada v. Teamsters*, [2004] 136 L.A.C. (4th) 102 (Can.).

39. *Id.* at paras. 3, 39 ("[T]he definition of 'commercial activity' under PIPEDA, while broad, is not in my view so wide-ranging that it encompasses the employment relationship itself and in particular the collection, use and disclosure of personal information *within* the organization.").

40. PIPEDA, S.C. 2000, c.5, Sch. 1, 4.3.4 (Can.); Arthur J. Cockfield, *Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance*, 29 QUEEN'S L.J. 364, 379 (2003).

41. R v. Spencer, [2014] 2 S.C.R. at paras. 68-74.

42. *Id.;* R. v. Ward, [2012] 112 O.R. (3d) 321, para. 46 (stating "PIPEDA does not create any police search and seizure powers" but "sets out the circumstances in which organizations may lawfully choose to disclose personal customer information, which must normally be kept confidential, to third parties including, in some circumstances, the police").

distinguish between content and non-content data.[43] Under the SCA, service providers can only voluntarily disclose non-content subscriber information except in emergencies, with the suspect's consent or pursuant to a court order or warrant.[44] Since PIPEDA's provisions does not make this distinction, Canadian courts assume the onus of gauging a user's privacy interest in particular types of information in a particular context.[45]

B. Constitutional Privacy Protections under Section Eight

Section Eight protects individuals from unreasonable searches and seizures.[46] Like other Charter provisions, Section Eight is the supreme law of Canada that renders null and void any federal or provincial laws inconsistent with it.[47] In *Canada v. Southam, Inc.*, the Supreme Court of Canada judicially interpreted Section Eight for the first time.[48] Taking into account the relatively mature American search and seizure law at the time, the Court elected to interpret Section Eight according to the "reasonable expectation of privacy" ("REP") test set forth in *Katz v. United States*.[49] In *Katz*, the United States Supreme Court held that a Fourth Amendment search occurs when law enforcement intrudes upon a subjective privacy expectation that society would find objectively reasonable.[50]

---

43. PIPEDA defines personal information as "information about an identifiable individual" not including "the name, title or business address or telephone number of an employee of an organization." S.C. 2000, c.5, 2(1). The SCA defines non-content data as:

> "(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number…."

Stored Communications Act, 18 U.S.C. § 2703(c)(2)(A)-(F) (2010).

44. 18 U.S.C. § 2702(c), 2703(a), (b). *See* Dan Grice & Dr. Bryan Schwartz, *Social Incrimination: How North American Courts Are Embracing Social Network Evidence in Criminal and Civil Trials*, 36 MAN. L.J. 221, 234-35 (2012) (stating that the SCA disclosure limitations are much stricter than PIPEDA's.).

45. PIPEDA, S.C. 2000, c.5, 2(1).

46. Canadian Charter of Rights and Freedoms, s 8, Part I of Constitution Act, 1982, *being* Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11.

47. Constitution Act, 1982, *being* Schedule B to the Canada Act, Part I, §52(1) (U.K.).

48. Canada v. Southam Inc., [1984] 2 S.C.R. 145 (Can.).

49. *Id.* at para. 24-26.

50. Katz v. United States, 389 U.S. 347, 351 (1961).

Canadian courts have consistently held that Section Eight imposes normative rather than descriptive constraints on law enforcement.[51] Thus, the reasonableness of a search or seizure is not dependent on the defendant's actual or constructive knowledge of the degree of privacy he enjoys.[52] Indeed, the Supreme Court of Canada has largely rejected the "risk analysis" that is prominently featured in Fourth Amendment jurisprudence.[53] In *R v. Sanelli*, for example, the Supreme Court of Canada held that law enforcement violated Section Eight when an undercover officer wearing a wire surreptitiously recorded an incriminating conversation with the defendant in the latter's apartment.[54] In so holding, the Court was careful to draw a distinction between a defendant's disclosure of incriminating information to a third party and law enforcement's recording of such information during the conversation.[55] While Section Eight does not protect individuals against "tattletales," it does prohibit law enforcement from covertly making warrantless recordings of a defendant's words and sharing those words with others.[56] In the latter scenario, the police unlawfully intrude upon the defendant's right to direct his words to particular individuals or groups.[57]

The Court reiterated this principle in *R v. Wong* when it held that law enforcement violated Section Eight when they cooperated with hotel staff to install a wire in a room the defendant publicly advertised and used

---

51. Whether the subjective element in the REP test has any independent significance is unclear. A simple thought experiment will frame the issue. Suppose the government provides the public advanced warning that it intends to conduct comprehensive electronic surveillance that day. *See* United States v. Kim, 415 F.Supp. 1252, 1256-57 (D. Haw. 1976). If a defendant viewed the broadcast and is later arrested that day, he or she cannot assert a subjective privacy interest in items revealed through electronic surveillance. *Id.* However, this outcome would clearly conflict with the stated purpose of Section Eight to provide normative constraints on law enforcement. *See* R. v. Tessling, [2004] 3 S.C.R. 432, para. 42 (Can.) ("The *subjective* expectation of privacy is important but its absence should not be used too quickly to undermine the protection afforded [Section Eight] to the values of a free and democratic society.").

52. Recent Canadian opinions suggest that the subjective prong of the REP test has been reduced to a factor in the objective test. In *Spencer*, the Court stated that the REP test depends on weighing a "large number of interrelated factors" that include factors "related to the nature of the privacy interest" and factors that directly measure the expectation of privacy "both subjectively and objectively." Spencer, [2014] 2 S.C.R, para. 18. Professor Orin Kerr has argued that the *Katz* court intended a subjective expectation of privacy to signify the loss of privacy interests when a person discloses information to a third-party. Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015). When such a disclosure occurs, at least under American law, the party assumes the risk that a third-party will disclose that information to law enforcement. *Id. See also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974); Alexandre Genest, *Privacy as Construed During the* Tessling *Era: Revisiting the "Totality of t- he Circumstances Test," Standing and Third Party Rights*, 41R.J.T. 337, 350-58 (2007).

53. *See* supra note 14; *compare* R v. Sanelli, [1990] 1 S.C.R. 30, paras. 14-19 (Can.) (rejecting the third-party risk analysis of Fourth Amendment jurisprudence) *with* United States v. White, 401 U.S. 745, 752 (1971); Smith v. Maryland, 442 U.S. 735, 744 (1979).

54. Sanelli, [1990] 1 S.C.R., para. 4.

55. *Id.* at paras. 23-24.

56. *Id.* at paras. 30-32.

57. *Id.*

as an illegal gaming house.[58] The lower court denied that a search had occurred because the defendant could not reasonably expect he would be left alone after he extended indiscriminate invitations to the public.[59] The Supreme Court of Canada, however, found that the surveillance violated Section Eight.[60] It reasoned that a hotel room is a context in which members of the public would feel secure from surveillance.[61] Moreover, the Court reaffirmed the holding of *Sanelli* when it stated that an intrusion of a heightened magnitude occurred when police made recordings of the defendant's spoken words. [62]

Sanelli and *Wong* are notable attempts to detach an individual's privacy rights with his or her status as a property owner. In *Sanelli* the defendant lacked a cognizable property interest in the apartment where the officer recorded the conversation[63] and in *Wong* the defendant kept his hotel room largely open to the public and used it as a "floating gambling house." [64] While these decisions generally support a notion of Section Eight as a personal rather than property right, the privacy interests at stake are nonetheless tethered to discrete spaces like the telephone booth in *Katz*.[65] Orin Kerr has noted that, despite rhetoric that the REP test exists independently of property rights, courts have been "fairly consistent" in anchoring privacy norms to privacy zones limited by clear geographical boundaries.[66] Judicial adherence to interpreting Section Eight in terms of privacy zones is not merely a product of slow changes in law. Rather, it reflects the limited ability of judges to determine a right to exclude—a critical facet of privacy law— without identifying tangible property over

58. R v. Wong, [1990] 3 S.C.R. 36 (Can.).

59. *Id.* at para. 17.

60. *Id.* at para. 24.

61. *Id.* at paras. 20-21.

62. *Id.* at para. 23. R v. Russell, [2012] BCSC 652, paras. 34-35 (Can.) ("Section 8 of the *Charter* is directed to the protection of the security of the person, not the protection of his property."); R v. Belnavis [1996], 29 O.R. (3d) 321, para. 38 (Can. Ont. C.A.).

63. Sanelli, [1990] 1 S.C.R. at para. 4.

64. Wong, [1990] 3 S.C.R. at para. 2.

65. *See* R. v. Edwards, [1996] 1 S.C.R. 128, paras. 47-48 (Can.) (finding that police did not violate defendant's privacy rights when they searched his girlfriend's apartment without a warrant because he was "just a visitor" at that apartment and did not "contribute to the rent or household expenses"); David J. Schwartz, *Edwards and Belnavis: Front and Rear Door Exceptions to the Right to be Secure from Unreasonable Search and Seizure* (1997)
10 C.R. (5th) 100 (stating that *Edwards* contradicts the Supreme Court of Canada's earlier precedent suggesting that "a reasonable expectation of privacy is not linked to the ability to assert a property interest in the place searched or property seized").

66. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 826-27 (2004). "One virtue of the Fourth Amendment's property-rights baseline is that it keeps easy cases easy." Florida v. Jardines, 133 S.Ct. 1409, 1417 (2013); Renee M. Pomerance, *Redefining Privacy in the Face of New Technologies: Data Mining and the Threat to the 'Inviolate Personality*,' 9 CAN. CRIM. L. REV. 273, 290-92 (2005).

which a person can exercise control.[67] In the absence of a privacy zone, reasonable expectations of privacy in each circumstance become difficult to resolve as well as difficult to articulate as precedent for future cases.[68]

R v. Cole is a notable attempt of the Court's effort to extend privacy rights beyond physical spaces.[69] In that case, the defendant was a teacher who accessed child pornography from a work-issued laptop.[70] After a school computer technician discovered the pornography, the principal seized the defendant's laptop and handed the hard drive over to the police.[71] The computer policy at the school allowed employees to use laptops both for work and "incidental personal use."[72] While the Court acknowledged the school's ownership of the laptop, the defendant claimed that the seizure of the laptop without a warrant violated Section Eight.[73] The Court agreed, finding that the police violated Section Eight when they searched the hard drive.[74] Unlike in *Sanelli* where the defendant divulged the incriminating information within a circumscribed area (i.e. an apartment),[75] the defendant in *Cole* accrued an incriminating search history from his usage of the laptop in diverse locations.[76] The breach of Section Eight, therefore, occurred not from an intrusion on a privacy zone but from the intrusion on the defendant's right to personal autonomy over sensitive information.[77] In the context of information privacy, the Court stated that the greater the extent to which the

---

67. *See* Edwards, [1996] 1 S.C.R. at 45 (considering whether defendant had "right to admit or exclude others from the place" in determining "reasonable privacy expectation"). *See* R v. Plant, [1993] 3 S.C.R., paras. 30-31.

68. *See* Elizabeth Paton-Simpson, *Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places*, 50 U. TORONTO L. J. 305, 330 (2000) ("By transcending the limits of sensory perception, technology has almost limitless potential to contravene normal expectations of privacy in both public and private places.").

69. R v. Cole, [2012] 3 S.C.R. 34 (Can.).

70. *Id.* at paras. 3-5.

71. *Id.*

72. *Id.* at para. 4.

73. *Id.* at paras. 50-51, 65-66. As Karen Eltis notes, *Cole* was a departure from prior case law that had considered the defendant's ownership in the property dispositive as to the issue of whether the defendant had a cognizable privacy interest. Karen Eltis, *Piecing Together Jones, A.B. and Cole: Towards a "Proportional" Model of Shared Accountability in Workplace Privacy*, 18 CANADIAN LAB. & EMP. L.J. 493, 507 (2014).

74. Cole,[2012]3S.C.R.,paras.81

75. Sanelli, [1990] 1 S.C.R., para. 4.

76. R. v. Cole, [2011] 105 O.R. (3d) 253, para. 16 (overruled by Cole, [2012] 3 S.C.R. at 34) ("Teachers were permitted to use their computer for personal use and to take it home during weekends and vacations.").

77. Cole, [2012] 3 S.C.R. at paras. 45-46. The protection of privacy as autonomy rests at the intersection of Section Seven and Section Eight of the Charter. Section Seven guarantees the right "to life, liberty and security of the person." Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, at §7 (U.K.). In *R v. Mortgentaler*, Justice Wilson interpreted this provision to "guarantee[ ] to every individual a degree of personal autonomy over important decisions intimately affecting their private lives" and that the "security of the person" extends to the individual's psychological integrity. [1988] 1 S.C.R. 30, para. 299 (Can.) (Wilson, J. concurring).

information constitutes a "biographical core of personal information," the more suspect the intrusion becomes under Section Eight.[78]

While *Cole* expanded privacy zones outward from a concrete space, its holding is somewhat limited because the Court found that only the police processing of the data violated Section Eight.[79] Citing the "statutory duty" of the principle to "maintain a safe school environment," the Court found that administrators did not violate Section Eight when they seized the defendant's laptop and searched its contents.[80] Moreover, the Court held that the administrators would not have acted improperly by informing police of their findings, thereby allowing the police to obtain a search warrant for the data.[81] While Section Eight imposes restraints only on state actors, Canadian courts have defined broadly the instances in which a private actor acts as a state agent.[82] The Supreme Court of Canada has found that school administrators "constitute a part of government" and thus Section Eight protections apply.[83] Schools, however, are also special environments that are subject to lesser privacy protections.[84] Thus, it is unclear how the Court would have treated the administrator conduct outside the context of education.

R v. Cuttell provides some guidance.[85] In that case, the Ontario Court of Justice held that a service provider that gave police the name and address of a defendant suspected of sharing child pornography violated the defendant's Section Eight right.[86] Because the address and name of the defendant constituted core private information, police could not use a service provider as a proxy for an intrusive search that the police could not otherwise conduct without a warrant.[87] So long as a service provider performed what essentially amounted to a governmental function (i.e. voluntarily cooperating with police in a criminal investigation), the service

78. Cole, [2012] 3 S.C.R., paras. 46-59. "The fact that the school board had acquired lawful possession of the laptop *for its own administrative purposes* did not vest in the police a delegated or derivative power to appropriate and search the computer *for the purposes of a criminal investigation*." *Id.* at para. 67*; see* Plant, 3 S.C.R., paras. 27-28.

79. Cole, [2012] 3 S.C.R., para. 73.

80. *Id.* at para. 62.

81. *Id.* at para. 73.

82. *See* Cuttell, [2009] 247 C.C.C. (3d), para. 50. ("[W]hen the police request private information from a third party such as an ISP in a criminal investigation, the ISP may well become an agent of the state whose decision to disclose information will be subject to scrutiny under s.8 of the *Charter*.").

83. *See* R v. M. (M.R.), [1998] 3 S.C.R. 393, paras. 24-25 (Can.).

84. "Teachers and administrators must be able to respond quickly and effectively to problems that arise in their school. When a school official conducts a search of or seizure from a student, a warrant is not required. The absence of a warrant in these circumstances will not lead to a presumption that the search was unreasonable." *Id.* at para. 45.

85. Cuttell, [2009] 247 C.C.C. (3d) at paras. 50, 55.

86. *Id.* at para. 59.

87. *Id.* at paras. 5-12, 59.

providers' disclosures of personal information to the police is the equivalent of a state action under Section Eight.[88]

Because service provider employees are subject to Section Eight constraints, Canadian courts have begun to factor the terms of agreements between users and service providers into the REP analysis.[89] In *R v. Gomboc* the Court addressed whether law enforcement were entitled to obtain data regarding electrical output at a home suspected of being used as a marijuana growing site without a search warrant.[90] The police requested the electrical data from the utility provider pursuant to a municipal ordinance that required providers to disclose information "to a peace officer for the purpose of investigating an offence if the disclosure is not contrary to the express request of the customer."[91] Since the defendant in *Gomboc* had not opted out of the disclosure provision, the Crown argued that he had no reasonable expectation of privacy with respect to his utility information.[92] The Court accepted this argument with some qualification.[93] Due to the "multitudinous forms of information" that comprise utility agreements and the limited opportunity for consumer bargaining, the Court decided to treat the terms as persuasive rather than dispositive of relative privacy rights.[94] Additionally, the Court found that the defendant did not have a strong privacy interest in electrical consumption data because the information did not reveal intimate details of the defendant's life.[95]

---

88. *Id.* at para. 50. *See also* Royal Bank v. Welton, [2008] 89 O.R. 3d 532, paras. 49-51 (Can. Ont. C.A.) (finding that, while the sharing of information between private entities is not restricted by Section Eight, a private entity's sharing of information to police can constitute a breach of Section Eight).

89. *See* Cole, [2012] 3 S.C.R., para. 52; Spencer, [2014] 2 S.C.R., paras. 53-67*;* Gomboc, [2010] 3 S.C.R. *passim;* R v. Cuttell, [2009] 247 C.C.C. (3d) *passim*; R v. Mahmood, [2008] 236 C.C.C. (3d) *passim*.

90. Gomboc, [2010] 3 S.C.R., paras. 1-2.

91. *Id.* at para. 31.

92. The *Gomboc* Court's analysis is a clear example of the oft-cited circularity of the reasonable expectation of privacy test. The Court states that the law recognizes that a person does not have a reasonable expectation of privacy in the utility information because utilities are subject to extensive regulation. *See* Renee M. Pomerance, *Shedding Light on the Nature of Heat: Defining Privacy in the wake of* R. v. Tessling, (2004), 23 C.R. (6th) 229, at 3; Richard Posner, *The Uncertain Protection of Privacy by the Supreme Cour*t, 1979 S.CT. REV. 173, 188 ("And it is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is."). While the Court aims at creating normative rather than descriptive privacy protections, its analysis depends on the state of the law at the time to elect the appropriate normative constraints. American search and seizure law shares this same logical inconsistency. For example, in *California v. Carney*, the Supreme Court of the United States justifies the reduced privacy expectations in an automobile in party by the "pervasive regulation of vehicles capable of traveling on the public highways." 471 U.S. 386, 392 (1985).

93. Gomboc, [2010] 3 S.C.R., paras. 32-33.

94. *Id.*

95. *Id.* at paras. 42-43.

In *Spencer* the Court expressed reservation about deferring to legislation when assessing the reasonableness of a search.[96] The Court eschewed an analysis that would treat PIPEDA as a core variable in assessing a reasonable expectation of privacy.[97] Because the purpose of Section Eight is to impose a check on legislative power, PIPEDA cannot be used as a factor to weigh against the existence of a reasonable expectation of privacy.[98] However, the Court in *Gomboc* noted that the legislative and contractual framework may be a persuasive consideration in determining whether there is a reasonable expectation of privacy.[99] In regards to contractual provisions, the Court additionally noted hesitation when such terms were vague and operated as essentially contracts of adhesion.[100] However, both *Spencer* and *Gomboc* leave unclear the precise relationship of search and seizure law with existing legislation and contractual obligations.

PART II: ANALYSIS

Informational privacy raises unique questions in search and seizure law. Most importantly, it is unclear whether the REP test is even workable in the data privacy context.[101] Resolution of this question is necessary before addressing the broader issue regarding the appropriate normative constraints of Section Eight and PIPEDA.

Section Eight data privacy cases have reiterated the importance of enforcing norms independent of existing legal obligations.[102] For this reason, the Supreme Court of Canada has eschewed strict reliance on property rights and rejected an interpretation of PIPEDA allowing legislatures to unilaterally draw privacy boundaries.[103] Instead the Court has sought to protect data privacy rights by weighing several factors

---

96.

> The reasonable expectation of privacy standard is normative rather than simply descriptive… Thus, while the analysis is sensitive to the factual context, it is inevitably "laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy."

Spencer, [2014] 2 S.C.R. at 18-19 (quoting R v. Patrick, [2009] 1 S.C.R. 579, para. 14 (Can.)).

97. *Id.* at para. 54 ("There is no doubt that the contractual and statutory framework may be relevant to, but not necessarily determinative of whether there is a reasonable expectation of privacy.").

98. *Id.* at paras. 62-63.

99. *Id.* at para. 54.

100. *Id.*

101. Orin Kerr has taken the position that *Katz* is an unworkable model in the data privacy context. Instead of relying on judicially imposed normative constraints, Kerr has argued that data privacy should be largely left to legislatures. Kerr, *supra* note 66, at 858-60.

102. *See* Spencer, [2014] 2 S.C.R., para. 18.

103. *See* Spencer, [2014] 2 S.C.R., paras. 53-55.

including, most importantly, the extent to which the information would tend to reveal a "biographical core of information."[104] While this approach acknowledges the reality that digital records can be as sensitive as information gleaned through a physical search of a home, it nonetheless suffers from an arbitrariness similar to the divining of privacy expectations from property rights.[105] Both *Cole* and *Spencer* emphasize that people have a privacy right in their use of technologies that ordinarily involve divulging personal information.[106] This normative lens, however, is both over- and under-inclusive. For example, a person who uses such technologies to broadcast every detail about his personal life—including his or her criminal conduct—would be protected under Section Eight, even though such transparency is not normal.[107] Conversely, a particularly private person may share data online that he or she, but not a reasonable person (as determined by the Court), believes is sensitive.[108] In both these cases Section Eight might fail to account for the intrusiveness of a given search.[109]

The disparity between actual and normative privacy practices is particularly egregious in the data privacy realm. Physical property has concrete boundaries that make instances of trespass readily identifiable.[110] No one would question, for example, that a Section Eight seizure occurs when officers carry off a defendant's computer. Moreover, even in cases in which courts must weigh relative property interests among several owners, the diversity of norms is nowhere near as immense

---

104. *Id.* at para. 27.

105. *See* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 348 (2012)):

> Estimating the frequency of technological surveillance practices is essentially impossible for most people (including most judges). Surveillance practices tend to be hidden, and few understand the relevant technologies… Some people will guess that privacy invasions are common. Others will guess that they are rare. But exceedingly few will know the truth, which makes probabilistic beliefs a poor basis for Fourth Amendment protection.

106. *See* Cole, [2012] 3 S.C.R. *passim*; Spencer, [2014] 2 S.C.R. *passim*.

107. *See* Abril, *supra* note 12, at 698.

108. *See id.*

109. *See id.*

110. *See* Gianclaudio Malgieri, *"Ownership" of Customer (Big) Data in the European Union: Quasi-Property As Comparative Solution?*, 20 No. 5 J. INTERNET L. 3, 10-11 (2016):

> Creating a property right around a *res* necessarily requires determining the boundaries of the *res* that is being endowed with exclusionary significance. While defining the *res* in relation to tangible resources poses few problems, defining the boundaries of the *res* in relation to intangibles is a difficult exercise that involves significant administrative and judicial costs. Hence, a key problem will be that vesting a property right in personal data implies that "someone" must define precisely what is worth a property right."(citations omitted).

See also Sonja R. West, *The Story of Us: Resolving the Face-off Between Autobiographical Speech and Information Privacy*, 67 WASH. & LEE L. REV. 589, 615-18 (2010).

as the variety of information-sharing habits among modern technology users.[111] The defendant in *Cole*, for example, might have used his workplace laptop primarily to view child-pornography or to split his time between viewing child-pornography and sending personal communications to his family.[112] In either case, the presumption that a work-issued computer contains data revealing a core of sensitive information might miss the mark.[113]

Canadian courts have responded to norm variance in informational privacy rights in part by transitioning to a more descriptive analysis of privacy expectations.[114] Thus, in *Gomboc* the Court found the regulatory scheme that governed the disclosure of electrical data persuasive.[115] If Section Eight ought to provide independent constraints on intrusive investigative practices, deference to existing legislation runs the risk of validating rather than curtailing legislative abuses of privacy rights.[116] PIPEDA, for example, contains numerous law enforcement exceptions that dramatically limit user privacy rights against private service providers.[117] Judicial deference to these exceptions would dramatically limit the scope of privacy rights users can retain against the government.

Though the current judicial treatment of information privacy is flawed in the information privacy context, the REP test can be salvaged provided courts develop a privacy model flexible enough to respond to variance in privacy norms.[118] Indeed, "reasonable expectation of privacy" is a mutable term and can be molded quite easily to a variety of frameworks.[119] While some scholars, including Kerr, have expressed concern that courts are less capable than legislatures in keeping up with privacy trends against a background of rapid technological change,[120] the languid pace of privacy legislation weighs against reducing the role of courts in enforcing privacy boundaries.

---

111. *See* Abril, *supra* note 12, at 698; Solove, *supra* note 11, at 41-42.

112. *See* Cole, [2012] 3 S.C.R. *passim*.

113. *See* R. v. Fearon, [2014] 3 S.C.R., para. 54 ("So we must keep in mind that the real issue is the potentially broad invasion of privacy that may, *but not inevitably will*, result from law enforcement searches of cell phones."); *see also* Riley, 134 S.Ct. at 2496-797 (Alito, J., concurring) (noting the lack of nuance in the rule that police may seize a cellphone incident to an arrest but cannot search its contents without a warrant).

114. Gomboc, [2010] 3 S.C.R., para. 31; Spencer, [2014] 2 S.C.R., paras. 53-67.

115. *Id.*

116. *See* Mayeda, *supra* note 7, at 46-48.

117. *Id.*

118. *See* Ric Simmons, *Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment,* 36 HARV. J.L. & PUB. POL'Y 549, 589-90 (2013) (rejecting a privacy law framework that would freeze the *Katz* doctrine in its current form and allow legislation to handle future privacy issues because "the reasonable expectations standard is meant to be a flexible one" and "ought to adjust as the amount of privacy that we expect evolves") (internal quotations omitted).

119. *Id.*

120. *See* Kerr, *supra* note 66, at 858-60.

Some scholars have argued that courts should enforce data privacy rights through a modified property framework.[121] As previously mentioned, The EU Directive and PIPEDA omit any mention of who owns personal data.[122] Instead, the enactments simply govern the circumstances under which service providers can disclose certain types of personal information.[123] The appeal of a property model for data privacy rests in the strength of the remedy.[124] Unlike liability rules in contract law, property law affords an owner injunctive relief when trespass occurs.[125] Such relief would restrict service providers from weighing ex ante the costs and benefits of personal data disclosure.[126] Since property rights track the user's intent to control, they are intimately linked to the owner's freedom against unwarranted intrusion.[127] Finally, since Canadian courts arguably still conceptualize privacy in terms of discrete, geographically limited zones,

---

121. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data,* 117 HARV. L. REV. 2055, 2094-96 (2004) (propounding a "hybrid inalienability" model of data privacy that allows users "to share, as well as to place limitations on, the future use of their personal information"); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-64 (1999) (presenting a property-based model of data privacy in which people own their data and can negotiate the price at which they are willing to relinquish the privacy in that data).

122. *See* Maxiener, *supra* note 29. The EU recently adopted the General Data Protection Regulation to replace the Directive. The regulation recognizes several property entitlements in data including the "right to be forgotten" and the "right of portability." Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), arts. 17-18, 2016 (O.J. (L 119) 1, available at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf; Its provisions will come into effect on May 25, 2018. *Id.* at art. 99; *see also* Malgieri, supra note 110, at 3, 6.

123. *See* Maxeiner, *supra* note 29, at 97; Nisker, *supra* note 23, at 318.

124. For a thorough explanation of the distinctions between property and liability remedies, see Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV.L.REV.1089, 1090-91 (1972).

125. *See Id.* Vera Bergelson argues that such relief could take the form of damage awards above the amount of actual damages. *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379 (2003). This could take the form of a per diem fine or, in the case of an unauthorized transfer of personal information, a fixed penalty amount. *Id.*

126. *See* Jane B. Baron, *Property As Control: The Case of Information*, 18 MICH. TELECOMM. & TECH. L. REV. 367, 380-81 (2012) ("Because a property rule would bar use of personal information without prior negotiation, it provides exactly the sort of control that has been sought to counteract the dystopia of ubiquitous-but-secret information flows."); Mark A. Lemley, *Contracting Around Liability Rules*, 100 CAL. L. REV. 463, 484 (2012) ("Property rules are all-or-nothing results; they don't allow the sorts of tailoring that liability rules do. In other words, a property rule sacrifices the potential accuracy of liability rules in the hopes of creating better ex ante incentives.").

127. For a more thorough explanation of the relationship between property and freedom, see Nadav Shoked, *The Duty to Maintain*, 64 DUKE L.J. 437, 446-53 (2014):

> To effectuate this innate capacity for choice immune from the interference of others, external objects of choice must be accessible to the individual. Therefore, each person must have an entitlement to external objects: a right rendering an object available for the exclusive exercise of her capacity for choice. In other words, holding an asset, whose manner of use cannot be dictated to the individual by others, is a prerequisite for the individual's freedom.

(citations omitted).

the conceptual underpinnings of a property-based model might already be in place.[128]

A property model of data privacy suffers from several disadvantages. First, it could have the unintended effect of exacerbating data privacy dilemmas by allowing users to sell their rights to personal information without understanding the privacy implications.[129] Because one of the core sticks in the bundle of property rights is freedom of alienation, a user might have no recourse to stop a buyer's re-sale of the data to unintended third parties.[130] Paul Schwartz has proposed a "hybrid alienability model" that would permit people to freely alienate personal data but retain an option to block further transfers of that data to "unaffiliated entities."[131] The problem with this model is that it is unduly inefficient when the information is sold to entities far-removed from the original sale.[132] Moreover, limited transferability would undoubtedly raise service provider costs and would thus undermine the ability of some people to value convenience more than privacy.[133]

A second disadvantage of the property model is that the contours of the property right are unclear. Concrete boundaries of traditional property ensure that owners can make transactions without encountering substantial confusion over the rights exchanged.[134] Such transparency is almost entirely absent in the information privacy context. Because even seemingly innocuous data might be aggregated into full-scale profiles, users would likely misjudge the scope of the personal information they disclose.[135] The lack of clear property boundaries in data also raises the question about

---

128. *See* Kerr, *supra* note 66, at 826-27.

129. *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1137-1138 (2000) ("Information privacy goals may not be achievable unless the default rule of the new property rights regime limits transferability."); *see also* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1303 (2000) (explaining the property model's "reliance on alienability and easy waiver tend to vest control over personal data in the data miner rather than the data's subject").

130. *See* Litman, *supra* note 129, at 1301:

> [P]rivacy is one of those things that many people don't believe they really need until they find themselves with something to keep secret. If easy assignment is the rule, they may no longer have the power to preserve their secrecy; even if they could, the exceptional nature of their asserting a privacy claim will tip off those from whom this is a secret that there is an interesting secret there. So, if someone who is deemed to have waived any property rights in the information supplied to businesses in return for product discounts should suddenly find himself diagnosed with hemorrhoids, or herpes, or HIV, he may have no practical way to recapture his secrecy.

131. *See* Schwartz, *supra* note 121, at 2059-60.

132. *See* Baron, *supra* note 126, at 381-82 ("If individuals have property rights to personal information, those individuals will determine as an initial matter whether to sell that information for money or barter it for services such as access to a website. But they will not be able to determine the use made of that information once it is in the hands of another.").

133. *See generally* Abril, *supra* note 12.

134. *See* Baron, *supra* note 126, at 380-85.

135. *Id.* at 381.

whether a property-rule could even work in practice.[136] If a service provider "trespasses" on personal information, it would be difficult to remedy the breach through an injunction when the core damage—exposing personal information—has already been realized.[137]

A privacy model based on contract law is a more effective alternative to regulating competing data privacy norms.[138] Because contract law allows people to negotiate and individualize the privacy rights they wish to retain, it would provide a much closer approximation of reasonable privacy expectations.[139] Many individuals who value convenience and publicity would negotiate for decreased privacy expectations, while those particularly keen on preserving private information would opt for higher privacy settings.[140] The former group would assume the risk that their communications would expose them to liability for misconduct and the latter group would relinquish some benefits of modern communication.[141] While Canadian courts have rejected a formal "risk analysis," the rejection has largely been directed towards assumption of hidden risks.[142] In such scenarios, the government deprives the individual of any meaningful ability to direct his or her communications to discrete individuals.[143] An opportunity to negotiate privacy expectations mitigates this risk, because the user can make an informed decision about the types of data that will reach people or entities.

The contract model has several advantages over a data ownership model. Because it governs rules for informational disclosure *ex ante,* a contract model avoids the vexing problem of determining the scope of the property right.[144] Unlike property law, contract law contains doctrines (e.g. unconscionability) that afford users more protection against

---

136. *See* Abril, *supra* note 12, at 707.

137. *Id.*

138. *Id.* at 706 ("Private rulemaking in the form of express user-to-user confidentiality contracts is perfectly tailored for the fickle concept of online privacy. After all, both privacy and contract are about self-determination.").

139. *Id.*

140. *Id.*

141. *Id.*

142. *See* Sanelli, [1990] 1 S.C.R., para. 24 ("A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning.").

143. *Id.*

144.

> When there is an information asymmetry, however, and one party knows more about the value of the property than another, or, as is even more common, the parties know their own valuations but not the valuation ascribed to the property by the other party, then it is likely that the property rule coupled with the information asymmetry may cause the parties to miss what would otherwise be an efficient "Coasean" trade. In such cases, liability rules may be more efficient.

Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 WM. & MARY L. REV. 1801, 1845-46 (2003) (citation omitted).

deceptive or manipulative practices.[145] In this way, contract law is better at "[taking] into account cognitive difficulties individuals may have in assessing the risks of certain transactions" as well as "[providing] protections to overcome these cognitive problems."[146]

The main obstacle to implementing a contractual-model of data privacy is that many service agreements afford users little room for negotiation.[147] In *Spencer* the court expressed reluctance about including contractual terms in the REP calculus because such agreements are often contracts of adhesion.[148] Absent the ability of users to freely negotiate, a contract could inaccurately match the privacy expectations of users with the actual privacy practices of service providers.[149] According to Karl Llewellyn, a standard form agreement creates two contracts: (1) a contract consisting of core terms that both parties freely negotiate and (2) a contract consisting of boilerplate terms a party does not read on the assumption the terms do not adversely affect the core terms.[150] Such contracts can only be valid if the boilerplate terms do not impair the meaning of the core terms and are not themselves unreasonable or unfair.[151]

But privacy policies tend to be so vague, complex and inconspicuous that ordinary users typically lack knowledge of the terms.[152] In part, this can explain the disconnect between popular desire for greater online privacy and actual consumer choices individuals make.[153] Thus while people are generally willing to pay a premium for more privacy in their transactions, few people are willing to read the boilerplate terms that are hallmarks of service provider contracts.[154] Under Llewellyn's model, those boilerplate terms are unfair when they distort the available information necessary to negotiate over core terms

145. *See* Samuelson, *supra* note 129, at 1156.

146. *Id.*

147. Mark MacAulay, *Contracts, Legislative Frameworks and the Reasonable Expectation of Privacy: Rethinking Section 8 in the Service Provision Context*, 20 CAN. CRIM. L. REV. 111, 131-132 (2015).

148. R v. Spencer, [2014] 2 S.C.R. 212, paras. 54-55 (Can.).

149. *See* MacAulay, *supra* note 147, at 131-132.

150. KARL L. LLEWELLYN, THE COMMON LAW TRADITION: DECIDING APPEALS 370 -371 (1960); *see* Shelley Smith, *Reforming the Law of Adhesion Contracts: A Judicial Response to the Subprime Mortgage Crisis*, 14 LEWIS & CLARK L. REV. 1035, 1097 (2010).

151. *Id.* at 371; *see* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453 (7th Cir. 1996) ("Terms of use are no less a part of 'the product' than are the size of the database and the speed with which the software compiles listings. Competition among vendors, not judicial revision of a package's contents, is how consumers are protected in a market economy.").

152. *See* MacAulay, *supra* note 147.

153. *See* Holland, *supra* note 11, at 893-94.

154. *See* Janice Y Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study,* 22 INFO. SYS. RESEARCH 254, 263 (2011); *see* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1434-36 (2011).

such as price.[155] The failure of service agreements to adequately signal privacy terms is a problem of incentives. Personal information is a valuable resource to service providers as the data affords marketers "unprecedented power to find new customers."[156] Service providers are unwilling to provide users increased privacy at the expense of economic benefit, at least when there is no clear signal increased privacy affects the demand for a product.[157]

One method to alter privacy practices is through regulations that force service providers to more clearly state privacy terms in standard form contracts.[158] Currently, PIPEDA's reasonableness standard places the burden on service providers to gauge whether their practices are compliant based on the totality of the circumstances.[159] Because of PIPEDA's lack of firm regulations, service providers can shift the burden on consumers to opt-out of intrusive data collection efforts.[160] Implementing a mandatory opt-in rule for service provider data collection could increase the likelihood users view and understand the privacy terms in their contracts.[161] Introducing a provision requiring service providers

155. Llewellyn, s*upra* note 150, at 370-371.

156. Jared S. Livingston, *Invasion Contracts: The Privacy Implications of Terms of Use Agreements in the Online Social Media Setting*, 21 ALB. L.J. SCI. & TECH. 591, 596 (2011); *see* Rubinstein, *supra* note 154, at 1439-40 ("[A]d targeting is valuable and privacy safeguards may increase opportunity costs to the extent that they diminish the economic value of online advertising, thereby creating an investment disincentive for firms dependent on advertising revenues.").

157. Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 HARV. J.L. & TECH. 149, 199-201 (2001) (explaining that, because providing greater privacy will, in the short term, forgo an immediate benefit, service providers must receive adequate signals from users to induce the entities to accept a short-term loss for a long-term gain).

158. As an example, the Federal Trade Commission has implemented regulations designed to prohibit contract terms that are "unfair and deceptive." Alan M. White, *Literacy and Contract,* 13 STAN. L. & POL'Y REV. 233, 258-59 (2002); *see* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 427-29 (2014) ("The adoption of transparency policies could allow companies to more freely operate while protecting consumers by allowing the FTC to bring enforcement actions when a promise of transparency is not upheld.").

159. *See* Fric, *supra* note 34, at 152.

160. *See* OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, Finding *Under the Personal Information Protection and Electronic Documents Act* (PIPEDA) (Apr. 7, 2015).

> It is important to note that while our Office's OBA Guidelines provide that opt-out consent may be appropriate in certain circumstances, they do not render opt-out consent the default for all behaviorally targeted advertising. In determining the appropriate form of consent, organizations should be careful to consider all of the circumstances surrounding their advertising programs, including those factors outlined in this report.

161. *See* Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 784-85 (2000). (explaining that the EU's recently passed General Data Protection Regulation mandates that service providers obtain express consent for data collection and use); *See* Art. 7, General Data Protection Regulation, 2012/0011 (COD). The consent of the "data subject," moreover, must be "freely given, specific, informed and unambiguous." *Id.* This is a modification of the previous data directive that allowed for implied consent under certain circumstances. *Id.* at art. 7 ("[T]he controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.").

to clearly and conspicuously state the types of data collected and the circumstances under which the data can be shared would increase use notice as well.[162] Finally, legislatures could mandate that service providers offer several tiers of privacy settings and enforce non-compliant providers with administrative penalties.[163] Under this scheme, service providers must pass on the opportunity cost they would incur from a reduction in data collection by increasing the service price for consumers who elect higher privacy options.[164] This scheme would fulfill what Richard Posner describes as the cost of privacy, or the cost society must bear when individuals decide to conceal their conduct from others.[165] Since affording people greater privacy protections in their communications might obfuscate their wrongdoing, the law can reduce this moral hazard by increasing the price of services for people who elect a high privacy preference.[166]

While regulation is needed to increase the visibility of privacy terms, Canadian courts should enforce Section Eight in a way that promotes greater bargaining over privacy terms. Thus, courts should assign more weight in the REP analysis to policies that are clear and allow users to opt-in to a variety of privacy options.[167] In making this analysis courts should avoid placing too much emphasis on the quantity of regulations as the Supreme Court of Canada did in *Gomboc*.[168] Obscure regulations, though numerous, are unlikely to signal users about privacy terms.[169] Instead courts should primarily consider whether an ordinary person reading the service agreement would be alerted to the privacy terms and have some opportunity to choose among privacy options.[170] In cases involving service agreements with unclear terms or lack of choice among tiers of privacy settings, courts should place little emphasis on contractual terms when assessing the reasonableness of the privacy expectation. Under these circumstances, it would be appropriate for courts to emphasize, as they currently do, the

---

162. *See supra* note 158 and accompanying text.

163. Karim Z. Oussayef, Note, *Selective Privacy: Facilitating Market- Based Solutions to Data Breaches by Standardizing Internet Privacy Policies*, 14 B.U. J. SCI. & TECH. L. 104, 109 (2008) (proposing mandated use of standard privacy policies that allow users to elect tiers of privacy settings at or above industry standards).

164. *Id.*

165. *See* Posner, *supra* note 13, at 233 ("The wish for privacy expresses a desire . . . to control others' perceptions and beliefs vis-a-vis the self-concealing person.").

166. *Id.*

167. Colleen McCullough argues that courts should determine the validity of boilerplate contracts in terms of their understandability. *Unconscionability As A Coherent Legal Concept*, Note, 164 U. PA. L. REV. 779 (2016). Under this model, the "offeror cannot impose on the offeree terms either that a reasonable person would not expect, or that, even if expected, would impose costs on third parties similarly situated to the offeree." *Id.* at 805.

168. *See* R. v. Gomboc, [2010] 3 S.C.R. 211, paras. 32-33 (Can.).

169. *See* R v. Spencer, [2014] 2 S.C.R. 212, para. 54 (Can.).

170. Gomboc, [2010] 3 S.C.R., paras. 32-33.

potentiality that the technology contains a biographical core of information.[171] This assumption might be wrong when measured against a defendant's usage habits, but it would provide at least some approximation of the privacy expectation.

CONCLUSION

Canadian data privacy law has struggled to adapt to the Big Data paradigm in which government and private actors collect and share personal information. PIPEDA—the primary data privacy statute—has accomplished little legislatively in restricting data sharing between law enforcement and service providers. Additionally, Courts have yet to adopt an adequate framework for assessing reasonable privacy expectations under Section Eight that recognizes wide-variations in data privacy norms. Because courts have typically only looked at the potentiality that technology will be used in certain ways, judges are apt to overlook the actual data privacy practices of individuals. By shifting towards a contractual expectation of privacy, Canadian courts can more adeptly handle the wide-variation in privacy norms and thus more accurately gauge reasonable privacy expectations. Accomplishing this transition will depend on increasing the opportunities for consumers and service providers to negotiate on privacy terms. Legislation that requires service providers to clearly state the terms of privacy policies and provide users a choice among privacy settings will increase the likelihood users will make an informed choice about the risks and benefits of exchanging data. Courts in turn ought to interpret compliant service provider agreements as highly persuasive in assessing the reasonableness of a search of data. In doing so they can better capture actual privacy expectations and thereby fulfill the purpose of Section Eight.

John D. Perry*

171. Spencer, [2014] 2 S.C.R., paras. 27-28.

* Staff Editor, Washington University Global Studies Law Review; J.D. (2017), Washington University School of Law; A.B. (2012), Princeton University.