2 The Reasonable Expectation of Privacy

I. Foundational Principles

Section 8 of the Charter guarantees everyone the right against unreasonable search and seizure by the state.[1] In so doing, section 8 functions as "a shield against unjustified state intrusions on personal privacy."[2]

Although section 8 is broad and its scope is ever growing,[3] there are natural limits to its growth. First, as with all Charter rights, section 8 provides protection only against state action.[4] A private actor might infringe another person's privacy and run afoul of the law in myriad ways, but the conduct of a private party, acting without any state involvement, will not amount to an infringement of section 8 of the Charter.

Second, section 8 does not protect against *all* state searches and seizures, but only against *unreasonable* ones. So not every investigatory technique used by the police or other state agency will trigger the application of section 8 of the Charter.[5] The touchstone of unreasonable searches and seizures is the *reasonable expectation of privacy*. A search or seizure is unreasonable only if the section 8 claimant enjoyed a reasonable expectation of privacy in relation to the place, thing, information, or body searched or seized.[6]

Section 8 of the Charter thus protects a claimant's reasonable expectation of privacy against unreasonable state intrusion.[7] The crux of every section 8 problem therefore begins with the question of whether the individual has a reasonable expectation of privacy in relation to the thing being searched or seized.

The difficulty in defining privacy—to say nothing of a reasonable expectation thereof—has proven challenging. In earlier times, one's expectation of privacy was co-extensive with one's property rights. "If the rights of private property were respected," Binnie J wrote in *R v Tessling*, "and the curtains of the home (or the drawbridge of the castle) were pulled, the King's agents could watch from a distance but would have no way of finding out what was going on inside."[8] But as technology developed, the protection afforded by property rights diminished. Seventeenth-century notions of privacy have given way to 21st-century realities. One's drawbridge and

1 See *Hunter v Southam Inc*, [1984] 2 SCR 145 at 159, 1984 CanLII 33.

2 *R v Kang-Brown*, 2008 SCC 18 at para 8.

3 See *R v Tessling*, 2004 SCC 67 at para 29 (noting that changes in technology may require the readjusting of our reasonable expectations of privacy).

4 Charter s 32 ("[t]his Charter applies … (a) to the Parliament and government of Canada in respect of all matters within the authority of Parliament including all matters relating to the Yukon Territory and Northwest Territories; and (b) to the legislature and government of each province in respect of all matters within the authority of the legislature of each province").

5 *R v Evans*, [1996] 1 SCR 8 at para 3, 191 NR 327, Sopinka J.

6 *Hunter v Southam Inc*, *supra* note 1 at 159-60 (emphasis added).

7 *Tessling*, *supra* note 3 at para 18. The test for "reasonable expectation of privacy" appears to originate in Harlan J's concurring opinion in *Katz v United States*, 389 US 347 at 360 (1967).

8 *Tessling*, *supra* note 3 at para 16.

castle will not protect you from wiretapping,[9] from forward-looking infra-red (FLIR) imaging,[10] from third-party production orders,[11] or from international mobile subscriber identity (IMSI) catchers.[12]

Under the modern conception of privacy, ownership remains relevant but not determinative of privacy rights.[13] As Dickson J noted in *Hunter v Southam Inc*, there is "nothing in the language of [section 8] to restrict it to the protection of property or to associate it with the law of trespass."[14] Section 8 of the Charter protects persons, not places or property.[15] It is, therefore, unnecessary to establish a proprietary interest in the place searched or the thing seized.[16]

II. The Edwards Test and the Totality of the Circumstances

How do we distinguish between information over which a reasonable expectation of privacy attaches and information that does not attract section 8 protection? The reasonable expectation of privacy analysis is fact-specific and contextual. The Supreme Court of Canada has emphasized that the assessment of whether one enjoys a "reasonable expectation of privacy" is to be made "in light of the totality of the circumstances of a particular case."[17] The Supreme Court has identified a non-exhaustive set of factors to be considered when assessing the totality of the circumstances:[18]

1. What was the nature or *subject matter* of the evidence gathered by the police?
2. Did the claimant have a direct *interest* in the contents?
3. Did the claimant have a *subjective expectation* of privacy in the informational content?

9 *R v Duarte*, [1990] 1 SCR 30, 71 OR (2d) 575.
10 *Tessling*, *supra* note 3 at para 16.
11 *R v Jones*, 2017 SCC 60.
12 See Nader R Hasan, "Searching the Digital Device" in Chan and Hasan, *Digital Privacy: Criminal, Civil and Regulatory Litigation* (Toronto: LexisNexis, 2018) at 3-5, citing Tamir Israel and Christopher Parsons, "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada" (Toronto: University of Toronto, 2016), online (pdf): <https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>.
13 *R v Cole*, 2012 SCC 53 at para 51, citing *Buhay*, 2003 SCC 30 at para 22.
14 See *Hunter v Southam Inc*, *supra* note 1 at 158.
15 *Ibid* at 158.
16 *Ibid*; *R v Dyment*, [1988] 2 SCR 417 at 426-27, 1988 CanLII 10, La Forest J; *Katz v United States*, 389 US 347 (1967).
17 *R v Edwards*, [1996] 1 SCR 128 at para 31, 26 OR (3d) 736; see also e.g. *R v Colarusso*, [1994] 1 SCR 20 at 54, 110 DLR (4th) 297; *R v Wong*, [1990] 3 SCR 36 at 62, 120 NR 34.
18 *Edwards*, *supra* note 17 at para 45, modified by *Tessling*, *supra* 3 at para 19, and *R v Patrick*, 2009 SCC 17 at para 27. See also *Cole*, *supra* note 13 at para 40; *R v Marakah*, 2017 SCC 59 at para 11.

4. If so, was the expectation *objectively reasonable*? In this respect, regard must be had to:
   a. the place where the alleged "search" occurred; in particular, did the police trespass on the claimant's property and, if so, what is the impact of such a finding on the privacy analysis?
   b. whether the informational content of the subject matter was in public view;
   c. whether the informational content of the subject matter had been abandoned;
   d. whether such information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality?
   e. whether the police technique was intrusive in relation to the privacy interest;
   f. whether the use of this evidence gathering technique was itself objectively unreasonable;
   g. whether the informational content exposed any intimate details of the claimant's lifestyle, or information of a biographic nature.

The Supreme Court has emphasized that this set of factors—often called the "*Edwards* factors"—is not exhaustive.[19] Depending on the nature of the privacy interests at stake, some factors will be more applicable than others.

The Supreme Court has repeatedly emphasized that the reasonable expectation of privacy standard is normative, not descriptive.[20] That is, the question is "what degree of privacy *should* we have?" not "what degree of privacy *do* we have?" As such, even though the claimant's subjective expectation of privacy may bolster their claim under the *Edwards* test, its absence is not fatal. Overemphasizing the individual's subjective expectation of privacy risks eviscerating privacy altogether. If a subjective expectation were all that is required, the state could unilaterally declare that henceforth all citizens would be subject to 24-hour surveillance in all of their daily activities and nobody would have a subjective expectation of privacy.[21] Such a result would be incompatible with democratic values. As the Court held in *R v Reeves*, "The question is not which risks the claimant has taken, but which risks should be imposed on him in a free and democratic society."[22]

Therefore, the reasonable expectation of privacy analysis "is 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

19 *Cole*, *supra* note 13 at para 45 (there is "no definitive list of factors that must be considered").

20 *R v Reeves*, 2018 SCC 56 at para 41; *Tessling*, *supra* note 3 at para 42.

21 *Patrick*, *supra* note 18 at para 14 ("[a] government that increases its snooping on the lives of citizens, and thereby makes them suspicious and reduces their expectation of privacy, will not thereby succeed in unilaterally reducing their constitutional entitlement to privacy protection").

22 *Reeves*, *supra* note 20 at para 41.

action for the protection of privacy."[23] The foundational question is not about the level of privacy we presently have (descriptive); the issue is: *what level of privacy should we expect from a society that purports to be free and democratic* (normative)?

III. The Subject Matter of the Search

Identifying the subject matter of the search is a key question in the *Edwards* analysis. The subject of a section 8 privacy claim may relate to the *person* (e.g., one's privacy interest in one's body or bodily integrity), to a *place or thing* (e.g., one's home or vehicle), to one's *information* (i.e., personal communications stored on a telephone), or any combination of the three. The privacy interests in a computer stored in one's home, for example, implicate both the territorial aspect of privacy (the home) as well as the informational aspect (the personal computer data). A "Fitbit,"[24] for example, involves both informational and bodily privacy because it tracks and records health information about one's body.

Defining the *subject matter of the search* is often a key issue, and can drive the ultimate section 8 analysis.[25] Care must be taken at this initial step to properly define the subject matter of the search. Chief Justice McLachlin set out the appropriate approach in *R v Marakah*:[26]

> The first step in the analysis is to identify the subject matter of the search. … How the subject matter is defined may affect whether the applicant has a reasonable expectation of privacy. Care must therefore be taken in defining the subject matter of a search … .
>
> The subject matter of a search must be defined functionally, not in terms of physical acts, physical space, or modalities of transmission. As Doherty J.A. stated in *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at para. 65, a court identifying the subject matter of a search must not do so "narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action."[27]

Marakah offers a helpful illustration on how defining the subject matter can drive the reasonable expectation of privacy analysis. In *Marakah*, the accused sent incriminating text messages to an accomplice named Mr Winchester. The police searched Mr Winchester's phone and sought to introduce the incriminating text messages that Mr Marakah had sent. Mr Marakah brought a section 8 application, arguing that he

23 *Patrick*, *supra* note 18 at para 14.

24 Fitbit is a brand of wireless-enabled wearable technology devices that measure data such as the number of steps walked, heart rate, quality of sleep, steps climbed, and other personal metrics involved in fitness.

25 For commentary, see David Schermbrucker, "Reasonable Expectation of Privacy Post-Spencer, Marakah/Jones" (April 2018), *Six-Minute Criminal Lawyer*, Law Society of Ontario.

26 *Supra* note 18.

27 *Ibid* at paras 14-15 (internal citations and quotations omitted).

had an ongoing reasonable expectation of privacy in the messages that he had sent to Mr Winchester but intended to keep private from the world at large. The Crown argued that he had no reasonable expectation of privacy in someone else's phone and hence lacked standing to challenge the search.

How the Court would define the subject matter of the search drove the reasonable expectation of privacy analysis. If the subject matter of the search is the phone, then the Crown's argument is compelling. It is difficult to argue that someone has a reasonable expectation of privacy in a piece of equipment that they do not own (and never have owned) and do not control (and never have controlled). If, on the other hand, the subject of the search is not the phone itself but the information stored on it, then the Crown's argument loses its force and issues like ownership and control of the digital device are a red herring.

The majority of the *Marakah* Court defined the "subject matter of the search" as the messages sent by Mr Marakah and received by Mr Winchester. Neither the phone itself nor its contents generally "is what the police were really after."[28] The correct characterization of the subject matter was therefore more properly "Mr. Marakah's electronic conversation with Mr. Winchester."[29]

There is intuitive appeal to this functional approach. Like most digital devices, the phone itself is just a conduit for the valuable information stored on it. This was not a situation where the police were interested in the physical device itself (e.g., for fingerprints left on the phone). The police were interested in Mr Winchester's phone only because they were interested in the electronic conversation that Mr Marakah had with him.[30]

IV. The Privacy Spectrum

Reasonable expectations of privacy exist along a spectrum—from low, to medium, to high. Where most or all of the *Edwards* factors point in favour of finding a reasonable expectation of privacy, the expectation may be high. Where the factors tug in opposite directions, the expectation of privacy may be diminished. Therefore, the inquiry as to whether an individual has a reasonable expectation of privacy is not an all-or-nothing proposition.

One should not be misled by the labelling of a reasonable expectation of privacy as "reduced" or "diminished." Those labels do not translate into "unimportant." A section 8 violation will still be established where an individual has a reduced expectation of privacy but where law enforcement fails to obtain a lawful authorization or to fit within an established exception to the warrant requirement.[31]

28 *Ibid* at para 17.
29 *Ibid*.
30 *Ibid* at para 20.
31 *Cole*, *supra* note 13; *Buhay*, *supra* note 13.

In *R v Cole*,[32] for example, the accused, a teacher at a school, was issued a work laptop that continued to be owned by the school board. School board policies provided that the data on work computers belonged to the school board, and network administrators had the ability to access files stored on the school computers when they were connected to the network. These facts weighed against a finding of privacy. But other factors, including that as a matter of practice, the teachers were allowed to use the school laptops for incidental personal use, and the highly personal and private nature of information stored on computers, weighed in favour of a reasonable expectation of privacy.[33] Given that the factors tugged in different directions, the Court concluded that the accused had a reasonable expectation of privacy but it was a "diminished" one.[34] The fact that it was a diminished expectation, however, did not obviate the need for the police to obtain a warrant, and the Court concluded that the police had infringed the accused's section 8 rights when they conducted a warrantless search of Mr Cole's school-issued laptop.[35]

Where an individual has a reasonable expectation of privacy at the low end of the spectrum, the lower expectation of privacy will inform the court's analysis on whether to exclude the information under section 24(2). This was the case in *Cole*. The Supreme Court of Canada unanimously agreed that the warrantless search violated the accused's section 8 rights, but held that exclusion of evidence under section 24(2) was not justified due in part to the diminished nature of Mr Cole's privacy rights.[36]

V. A Uniquely Canadian Approach: Rejection of the Third-Party Doctrine

The defining feature of the reasonable expectation of privacy test is its context-specific malleability. This contextual malleability is the natural outgrowth of the *Edwards* test, which focuses on the totality of the circumstances. The Supreme Court has eschewed rigidity and has repeatedly rejected attempts to introduce US doctrines into Canadian constitutional law. Although the reasonable expectation of privacy is a concept derived from US Fourth Amendment jurisprudence,[37] there are important conceptual differences between US and Canadian approaches, which have come to inform the Canadian analysis of the scope of section 8 of the Charter.

One such difference is Canadian courts' rejection of the "third-party doctrine," which is a prominent feature of US Fourth Amendment jurisprudence. The third-party doctrine posits that when an individual shares private information with a third

32 *Supra* note 13.
33 *Ibid* at para 49.
34 *Ibid* at para 58.
35 *Ibid* at para 79.
36 *Ibid* at para 92.
37 *Hunter v Southam Inc*, *supra* note 1 at 158-59, citing Harlan J's concurring opinion in *Katz v United States*, 389 US 347 at 360 (1967).

party, the individual no longer has a reasonable expectation of privacy in that information.[38] The doctrine is premised in part on a related concept, the "assumption of risk" doctrine—meaning that when an individual shares private information with a third party, that individual assumes the risk that the third party will share that information with others, including the state.[39]

The Supreme Court of Canada has rejected the third-party doctrine and the assumption of risk analysis. Instead, the Supreme Court has focused on the "totality of the circumstances" when deciding whether a reasonable expectation of privacy exists. Sharing information with third parties may impact on the ultimate expectation of privacy in the totality of the circumstances, but it will never alone be dispositive.

Thus, in *R v Duarte*,[40] the Court concluded that the recording of a conversation between the accused and an undercover officer wearing a bodypack violated section 8 of the Charter. In reaching this conclusion, the Court distinguished between the "tattletale" risk (the risk that someone will tell the police what you said) and the risk that someone will consent to the police making an electronic recording of your words.[41] As La Forest J wrote on behalf of the majority of the Court, "No justification for the arbitrary exercise of state power can be made to rest on the simple fact that persons often prove to be poor judges of whom to trust when divulging confidences or on the fact that the risk of divulgation is a given in the decision to speak to another human being."[42] The Court concluded that "[t]hese risks are of a different order of magnitude"—the tattletale risk is one that is reasonable to ask citizens to bear in a free and democratic society, whereas the surveillance risk is not.[43]

The Supreme Court reaffirmed (and arguably extended) this holding in *Reeves*. There, the accused's spouse consented to the police seizing a family-shared computer. The Court held that while it is reasonable to ask citizens to bear the risk that a co-user of their shared computer may access their data on it, and even perhaps discuss this data with the police, it is not reasonable to ask them to bear the risk that the co-user could consent to the police taking the computer and searching its contents.[44] In so holding, the Court underscored the normative nature of the reasonable expectation of privacy: "The question is not which risks the claimant has taken, but which risks should be imposed on him in a free and democratic society."[45]

The state does not get to piggy-back on the rights of access of third parties even if the third party accessed the goods or information lawfully. In *R v Buhay*, the Court

38 *United States v Miller*, 425 US 435 (USSC 1976).
39 See *US v Jacobsen*, 104 S Ct 1652 (1984).
40 *Supra* note 9.
41 *Ibid* at 48.
42 *Ibid* at 48-49.
43 *Ibid*.
44 *Reeves*, *supra* note 20 at para 41.
45 *Ibid* at para 41.

held that the police could not justify their warrantless search of the accused's belongings from his rented bus depot locker simply because the private security guards who had contacted the police had earlier gone into the same locker with a master key and searched the same belongings. The intervention of the security guards at the bus depot did not extinguish that privacy interest or "relieve the police from the *Hunter v Southam Inc* requirement of prior judicial authorization before seizing contraband uncovered by security guards."[46]

Likewise, in *R v Dyment*, the Court held that an accused continued to enjoy a reasonable expectation of privacy against the state with respect to a blood sample that had been lawfully obtained by a treating physician.[47] In *R v Wong*, the Court held that even though the accused invited members of the public to enter his hotel room, he continued to enjoy a reasonable expectation of privacy in the room's activities vis-à-vis the state.[48] In *R v Mercer*, the Ontario Court of Appeal, applying *Wong*, excluded evidence of cannabis residue and cash that had been seized from the accused's hotel room despite the fact that the police were permitted to enter the room by hotel staff, who had an undisputed right to enter the room.[49]

In *R v Colarusso*,[50] the Supreme Court held that the warrantless seizure of the accused's blood and urine samples by the police from the coroner could not be justified by either (1) the original consent of the accused to provide the samples to the hospital for medical purposes, or (2) the coroner's statutory authority to seize these samples from the hospital for the purpose of determining whether an inquest was necessary.

The rejection of the third-party doctrine has special currency when it comes to digital information.[51] After all, we cannot use our phones, access our emails, or browse the Internet without sharing private information with third-party telecommunications providers and Internet service providers (ISPs). It defies common sense to suggest that we abandon our expectation of privacy simply by using the tools that modern society demands of us.

As such, in *Cole*,[52] discussed above, school board policies provided that the data on work computers belonged to the school board and network administrators had the ability to access files stored on the computers when they were connected to the

46 *Buhay*, *supra* note 13 at paras 22, 33-34, 38.

47 *Dyment*, *supra* note 16 at 430-36.

48 *Wong*, *supra* note 17 at 52-55.

49 *Mercer*, 1992 CanLII 7729, [1992] OJ No 137 (QL) at paras 10-15, 24-36 (CA).

50 *Supra* note 17 at 60-61, 63, 66-67.

51 Although US scholars have been critical of the third-party doctrine for decades, the digital age has only underscored the doctrine's shortcomings. See e.g. Gerald G Ashdown, "The Fourth Amendment and the Legitimate Expectation of Privacy" (1981) 34:5 Vand L Rev 1289; Christopher Slobogin, "Subpoenas and Privacy" (2005) 54:3 DePaul L Rev 805 at 829.

52 *Cole*, *supra* note 13.

network. Yet, the fact that the school administration and school board could lawfully access the contents of the accused's computer and lawfully seize the accused's work-issued computer did not obviate the need for the police to obtain a search warrant in order to search the computer. A third party cannot waive another party's privacy rights.[53]

In *R v Spencer*, an officer of the Saskatoon Police Service was engaged in a child pornography investigation. Using the publicly available Limewire file-sharing software, he searched for users sharing child pornography. Limewire also permitted him to see the Internet Protocol (IP) addresses associated with each user. He ran a list of IP addresses against a database with approximate locations and found that one of the IP addresses had an approximate location of Saskatoon, with Shaw Communications Inc as the ISP.[54]

What he lacked, however, was a precise knowledge of where exactly the computer was and who was using it. He therefore made a request to Shaw under section 7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act*,[55] requesting the subscriber information associated with the IP address. No production order was obtained. Shaw complied with the request and provided their customer's name, address, and telephone number.

The question on appeal was whether section 8 demands that a warrant be sought and obtained to access Internet subscriber information. The Supreme Court held that it does.[56] The fact that the information sought was voluntarily surrendered to a third-party ISP was immaterial. If a reasonable expectation of privacy attached to that information (and the Supreme Court held that it does), then the surrender of that information to the ISP for purposes of providing Internet service does not surrender privacy vis-à-vis the state.[57] Therefore, the police needed a judicially authorized production order in order to access the information notwithstanding the purported statutory law-enforcement sharing provisions in PIPEDA. It was insufficient to simply make a law enforcement request of the telecommunications provider to get the subscriber information.

VI. Control Is Not Dispositive

The rejection of the third-party doctrine in Canada means that the element of *control* is not determinative of a reasonable expectation of privacy. Just because a third party may be in control (in whole or in part) of the information, premises, or thing over which we claim privacy, we may still have a reasonable expectation of privacy vis-à-vis

53 *Ibid* at para 76.
54 *Spencer*, 2014 SCC 43 at paras 7-12.
55 SC 2000, c 5.
56 *Spencer*, *supra* note 54 at para 45.
57 *Ibid* at paras 55-63.

the state. Thus, while "control" is a factor under the *Edwards* analysis, it is not—and has never been—dispositive.

The Supreme Court of Canada's decisions in *Marakah*[58] and *Reeves*[59] underscore this point. In *Marakah*, the accused sent incriminating text messages to his accomplice. The police searched the accomplice's phone and sought to introduce the incriminating text messages against Mr Marakah. The question was whether the accused had a reasonable expectation of privacy in messages *sent* by the accused but *stored on* the accomplice's phone. The accused had no property interest in the accomplice's phone, nor even a modicum of control over how the accomplice used his phone or to whom he forwarded the accused's messages. Still, the majority held that in the totality of the circumstances, the accused retained a reasonable expectation of privacy in the sent text messages.[60]

In so holding, the majority downplayed the importance of physical control of the device:

> First, control is not dispositive, but only one factor to be considered in the totality of the circumstances. Second, my colleague's approach focuses not on the subject matter of the search, the electronic conversation, but rather on the device through which the information was accessed, [the accomplice's] phone. Sometimes, control over information may be a function of control over a physical object or place. However, this is not the only indicator of effective control. Sometimes, as with electronic conversations, control may arise from the choice of medium and the designated recipient.[61]

Two aspects of this passage are salient. First, the Court emphasized that "the subject matter of the search" is the *digital information* and not the accomplice's phone itself. Second, the concept of "control" has been reconceptualized for a digital age. Control means choosing with whom you share your private messages. And by sharing messages or information with intended recipients, one does not by implication waive privacy as against the world at large.

The Supreme Court's decision in *Reeves* also downplays the element of control. At issue in *Reeves* was one spouse's consent for the police to search a family computer. The accused's common law spouse reported to authorities that there was child pornography on the family computer that she shared with the accused and provided consent to the police to seize and search it. The issue was whether the accused's spouse could waive his privacy interest in the shared computer. The Supreme Court held that she could not. One user of a shared computer cannot waive another user's reasonable expectation of privacy: "By choosing to share a computer with others, people do

58 *Marakah*, *supra* note 18.
59 *Reeves*, *supra* note 20.
60 *Marakah*, *supra* note 18 at paras 25-54.
61 *Ibid* at para 44.

not relinquish their right to be protected from the unreasonable seizure of it."[62] The Court found a section 8 violation and excluded the evidence found thereon.[63]

Writing for the majority, Karakatsanis J held:

> I cannot accept that, by choosing to share our computers with friends and family, we are required to give up our *Charter* protection from state interference in our private lives. We are not required to accept that our friends and family can unilaterally authorize police to take things that we share. The decision to share with others does not come at such a high price in a free and democratic society.[64]

Under the contextual "totality of the circumstances" test from *Edwards*, which necessarily balances an array of factors, ownership and control, though relevant, are not determinative of privacy rights.[65]

VII. Using the Crown's Theory to Establish a Reasonable Expectation of Privacy

The accused need not establish all of the *Edwards* factors through direct evidence. Indeed, in some cases, the accused may rely on the Crown's theory of the case to establish facts relevant to the reasonable expectation of privacy.

In *R v Jones*,[66] the accused brought a pre-trial application to exclude text messages obtained through a production order. Importantly, Mr Jones did not lead any evidence that he had authored the text messages.[67] Rather, he argued that he was entitled to rely on the Crown's theory that he was the author of the text messages, which in turn established a subjective expectation of privacy in the contents of the message. As a practical matter, this would avoid Mr Jones having to admit authorship of the text messages on the *voir dire* to establish a subjective expectation of privacy, which was tantamount to an admission of the *actus reus* of the offence on the trial proper. In contrast, the Crown argued that the burden remained with the claimant on a Charter *voir dire* and that this required the claimant to call evidence to ground standing and the Charter breach.

The trial judge in *Jones* accepted the Crown's argument and held that the appellant did not have standing to challenge the production order. She found that there was no evidence that the appellant had a subjective expectation of privacy in the text messages, or any evidence to suggest that such an expectation was objectively reasonable. The Ontario Court of Appeal upheld that finding on appeal.

62 *Reeves*, *supra* note 20 at para 37.
63 *Ibid* at para 61.
64 *Ibid* at para 44.
65 *Buhay*, *supra* note 13 at paras 22-23; *Cole*, *supra* note 13 at para 54; also *Marakah*, *supra* note 18 at paras 38-45; *Edwards*, *supra* note 17 at para 45(6)(iii).
66 *Supra* note 11.
67 *Ibid* at para 6.

The Supreme Court of Canada reached a different conclusion. Writing for a majority of the court, Côté J held that the accused was permitted to rely on the Crown's theory to establish that he authored the text messages and, in turn, to establish a subjective expectation of privacy in the messages. Justice Côté wrote:

> I conclude that an accused mounting a s. 8 claim may ask the court to assume as true any fact that the Crown has alleged or will allege in the prosecution against him in lieu of tendering evidence probative of those same facts in the *voir dire*. In this case, Mr. Jones should have been permitted to rely on the Crown allegation that he authored the Text Messages, and his subjective expectation of privacy in the subject matter of the search is accordingly established.[68]

Subsequently, in *R v Labelle*, the Court of Appeal for Ontario wrote that the holding in *Jones* was not limited to establishing a subjective expectation of privacy.[69] *Jones* stands for the broader proposition that "the accused can rely on the Crown theory to establish certain facts relevant to their s. 8 claim."[70]

VIII. Applying the Reasonable Expectation of Privacy Test

Although the reasonable expectation of privacy is a concept that defies tidy categories and will be driven by the totality of the circumstances pursuant to the fact-specific *Edwards* test, we have organized the discussion under three headings: (1) personal privacy, (2) territorial privacy, and (3) informational privacy.

A. Personal Privacy

It should be no surprise that we enjoy a high reasonable expectation of privacy over our bodies and bodily integrity. Searches of our bodies are inherently invasive and may even be humiliating and degrading.[71] Such searches may also reveal sensitive information that may be misused by authorities.[72] Respect for human dignity and individual autonomy requires that all searches invading one's bodily integrity be lawfully authorized.

The cases involving bodily searches generally fall into two categories: (1) searches of a person's body (e.g., pat-down searches, a strip search, body-cavity search), and (2) the seizure of bodily substances, impressions, and images.[73]

68 *Ibid* at para 9.
69 *Labelle*, 2019 ONCA 557 at para 31.
70 *Ibid* at para 31.
71 *Vancouver (City) v Ward*, 2010 SCC 27 at para 64; *R v Golden*, 2001 SCC 83 at para 83.
72 *Dyment*, *supra* note 16 at 432-34.
73 Steven Penney, Vincenzo Rondinelli & James Stibopoulos, *Criminal Procedure in Canada* (Toronto: LexisNexis, 2011) at 149.

1. Strip Searches

Strip searches "are inherently humiliating and degrading regardless of the manner in which they are carried out."[74] Nevertheless, the police have a limited common law power to conduct strip searches pursuant to their power of search incident to arrest.[75]

In order for a strip search to be justified as a search incident to arrest, it is necessary that the arrest itself be lawful.[76] A lawful arrest, however, is necessary but not sufficient. Routine strip searches are not justifiable. The fact that the police have reasonable and probable grounds to carry out an arrest does not confer upon them the automatic authority to carry out a strip search.[77] In addition to reasonable and probable grounds justifying the arrest, the police must establish reasonable and probable grounds justifying the strip search.[78]

Given the high degree of invasiveness, a strip search of the arrestee will only be justifiable where the police establish reasonable and probable grounds for a strip search for the purpose of discovering weapons or seizing evidence related to the offence for which the detainee was arrested.[79]

Where these preconditions to conducting a strip search incident to arrest are met, it is also necessary that the strip search be conducted in a *manner* that does not infringe section 8 of the Charter.[80] The search must interfere with privacy and dignity as little as possible. Generally, this means that strip searches (where justifiable) should only be carried out at the station.[81] Strip searches "in the field" should only occur where urgent and necessary.[82]

Police officers are expected to know that a "frisk" or "pat-down" search at the point of arrest will generally suffice for purposes of determining if the accused has weapons on their person.[83]

2. Frisk Searches

Frisk or "pat-down" searches of detainees are authorized under the *Waterfield* doctrine because of officer safety concerns—that is, the prospect that the detainee is in possession of a weapon.[84] Outside of this specific justification a frisk or "pat-down" search of a person's body will violate a reasonable expectation of privacy in most

74 *Vancouver (City) v Ward*, *supra* note 71 at para 64; *Golden*, *supra* note 71 at para 90.
75 *Golden*, *supra* note 71 at para 91.
76 *Ibid.*
77 *Ibid* at para 91. See also Chapter 10.
78 *Ibid* at para 92.
79 *Ibid* at para 99.
80 *Ibid* at para 94.
81 *Ibid* at para 102.
82 *Ibid.*
83 *Ibid* at para 92.
84 *R v Mann*, 2004 SCC 52; *R v Aucoin*, 2012 SCC 66.

contexts.[85] Frisk searches happen with regularity because we submit to them on consent (e.g., when entering a high-security building like a stadium) and also because we are deemed to have a lower or diminished expectation of privacy in certain contexts (e.g., airports and border crossings) because of the unique security and public interest concerns. These contexts are, of course, not police-inspired criminal investigations. In addition, the pat-down search upon lawful arrest will often be justifiable under the police power of search incident to arrest.[86]

3. Taking of Bodily Substances

The police cannot use medical personnel to do an end-run around section 8 of the Charter. Section 8 thus applies when police acquire bodily samples from medical personnel who have taken those samples for medical purposes.[87] The Supreme Court of Canada has been particularly vigilant of the police co-opting health care providers. As a society, we do not want people to have to choose between their legal rights and seeking medical treatment.[88]

There is typically no expectation of privacy in bodily samples that have been "abandoned."[89] Therefore, an accused who is not in custody who discards a tissue with mucous or a cigarette butt, or an accident victim who bled on their vehicle or on the side of the road,[90] generally does not have a reasonable expectation of privacy in those samples. Where, however, the accused is in custody, the situation is more complicated. In *R v Stillman*, the majority of the Court held that the accused did not abandon a mucous-containing tissue when he discarded it while in police custody.[91] He had previously refused to provide voluntary samples. Since people in police custody cannot altogether prevent the seizure of bodily substances, the Court held that the accused retained a reasonable expectation of privacy in the tissue and thus the warrantless seizure of the tissue violated section 8.[92]

4. Bodily Impressions

Compared to the taking of bodily samples, the taking of fingerprints is minimally intrusive. Taking one's fingerprints does not compare to a state agent inserting a needle in one's arm. That said, we do retain a reasonable expectation of privacy in our fingerprints. Legislation compelling accused persons to submit to fingerprinting has been

85 See *Mann*, *supra* note 84 at para 56.
86 *R v Caslake*, [1998] 1 SCR 51, 155 DLR (4th) 19; *R v Fearon*, 2014 SCC 77.
87 *Dyment*, *supra* note 16; *Colarusso*, *supra* note 17.
88 *R v Taylor*, 2014 SCC 50 at para 41; *R v Culotta*, 2018 ONCA 665, aff'd 2018 SCC 57.
89 *Stillman*, [1997] 1 SCR 607 at para 62, 185 NBR (2d) 1.
90 *R v LeBlanc*, [1981] NBJ No 273 (QL), 36 NBR (2d) 675 (CA).
91 *Stillman*, *supra* note 89 at para 62.
92 *Ibid.*

upheld as constitutional, but that lawful authority dissipates if the individual is acquitted or the charges are withdrawn.[93]

5. Penile Swabs

A penile swab does not fall within the scope of *Stillman*.[94] It is conceptually different because a penile swab is not designed to seize the accused's own bodily materials but rather the complainant's.[95] Second, according to a majority of the Supreme Court, the penile swab is in some ways less invasive than taking dental impressions and the forcible taking of parts of a person.[96] Third, unlike with the accused's bodily materials or impressions, evidence of the complainant's DNA degrades over time, so there is urgency.[97] Because of these differences, the balance struck between privacy and law enforcement interests is different from an accused's bodily samples and impressions.

The power to take a penile swab flows from the police's common law power to conduct a search incident to arrest.[98] The police may take a penile swab incident to arrest if they have reasonable grounds to believe that the search will reveal and preserve evidence of the offence for which the accused was arrested.[99] Relevant factors include:[100]

- the timing of the arrest in relation to the alleged offence,
- the nature of the allegations,
- the potential for destruction or degradation of the complainant's DNA, and
- whether there is evidence that the substance being sought has already been destroyed.

The swab must also be conducted in a reasonable manner. The following factors are relevant: [101]

- A swab should, as a general rule, be conducted at the police station.
- It should be conducted in a manner that ensures the health and safety of all involved.
- It should be authorized by a police officer acting in a supervisory capacity.
- The accused should be informed shortly before the swab of the nature of the procedure, its purpose, and the authority of the police to require the swab.

93 *R v Beare*, [1988] 2 SCR 387 at 414, 55 DLR (4th) 481.
94 *R v Saeed*, 2016 SCC 24 at para 51.
95 *Ibid* at para 48.
96 *Ibid* at paras 55-56.
97 *Ibid* at para 71.
98 *Ibid* at para 74.
99 *Ibid* at para 75.
100 *Ibid* at paras 75-77.
101 *Ibid* at para 78.

- The accused should be given the option of removing his clothing and taking the swab himself or the swab should be taken or directed by a trained officer or medical professional, with the minimum of force necessary.
- The officers carrying out the swab should be of the same gender as the accused unless the circumstances compel otherwise.
- There should be no more police officers involved in the swab than are reasonably necessary in the circumstances.
- The swab should be carried out in a private area.
- It should be conducted as quickly as possible and in a way that ensures that the person is not completely undressed at any one time.
- A proper record should be kept of the reasons for and the manner in which the swabbing was conducted.

While what constitutes a reasonable penile swab may vary with the facts of each case, the onus is always on the Crown to establish that the police had reasonable grounds to believe the swab would reveal the evidence sought and that the swab was conducted in a reasonable manner.[102]

B. Territorial Privacy

1. Dwellings and Private Property

Although the modern view holds that section 8 of the Charter protects people and not places, and that a property interest is not necessary for a reasonable expectation of privacy, the physical location of the privacy claimant continues to be important. As they have for centuries, people continue to enjoy a high reasonable expectation of privacy in their homes. Since *Semayne's Case* in 1604, it has been firmly established that "a man's home is his castle, and that even the King himself had no right to invade the sanctity of the home without the authority of a judicially issued warrant."[103]

The Supreme Court of Canada has repeatedly underscored the sacrosanct nature of the reasonable expectation of privacy in our homes:

> It is hard to imagine a more serious infringement of an individual's right to privacy. The home is the one place where persons can expect to talk freely, to dress as they wish and, within the bounds of the law, to live as they wish. The unauthorized presence of agents of the state in a home is the ultimate invasion of privacy. It is the denial of one of the fundamental rights of individuals living in a free and democratic society. To condone it without reservation would be to conjure up visions of the midnight entry into homes by agents of the state to arrest the occupants on nothing but the vaguest suspicion that they may be enemies of the state. This is why for centuries it has been recognized that a man's home is his castle.[104]

102 *Ibid* at para 83.
103 *Semayne's Case* (1604), 5 Co Rep 91, 77 ER 194.
104 *R v Silveira*, [1995] 2 SCR 297 at para 148, 1995 CanLII 89.

The sanctity of the home, however, does not mean that the police are powerless to enter the home absent a warrant. There are limited circumstances where the common law recognizes an implied licence for the police to enter a residential property.

One such exception is the implied licence to knock. The common law has long recognized an implied licence for all members of the public, including the police, to approach the door of a residence and knock.[105] This implied invitation, unless expressly disavowed, effectively waives the privacy interest that an individual might otherwise have in the approach of the door of their residence.[106]

The implied licence is limited to facilitating communication with the public for some valid public interest purpose. Where members of the public, including police, exceed the terms of this waiver, and approach the door for some unauthorized purpose, "they exceed the implied invitation and approach the door as intruders."[107] In *R v Evans*, when the police approached the residence to "sniff" for the presence of marijuana, the terms of the implied licence were exceeded and the search was unreasonable.[108]

A second such exception is an implied licence of state authorities to intrude on private property in response to an emergency.[109] That licence may include the power of forced entry into the home where the circumstances so require.[110]

Such an intrusion, however, must be narrowly tailored to its purpose: protection of life and safety. The implied licence to enter in response to an emergency does not authorize the police to conduct a further search of the residence.[111]

In *R v Jamieson*, the police lawfully entered the home under this implied licence. Once inside, they saw, in plain view, drug paraphernalia.[112] Because the entry into the home was lawful, seizure of the drug paraphernalia fell within the plain view exception to the warrant requirement.[113]

Where the police rely on a common law exception to justify a warrantless entry, they must satisfy the two-part test from *R v Godoy*:[114]

> [F]irst, does the police conduct fall within the general scope of any duty imposed by statute or recognized at common law; and second, does the conduct, albeit within the general scope of such a duty, involve an unjustifiable use of powers associated with the duty.[115]

105 *Evans*, *supra* note 5 at para 6; *R v Tricker*, 1995 CanLII 1268, 21 OR (3d) 575 at 579 (CA), citing *Robson v Hallett*, [1967] 2 All ER 407 (CA).
106 *Evans*, *supra* note 5 at para 6.
107 *Ibid* at para 14.
108 *Ibid* at para 17.
109 *Godoy*, [1999] 1 SCR 311, 168 DLR (4th) 257 [*Godoy* cited to SCR]; *Jamieson*, 2002 BCCA 411.
110 *Godoy*, *supra* note 109 at para 22.
111 *Ibid*.
112 *Jamieson*, *supra* note 109.
113 *Ibid*.
114 *Supra* note 109.
115 *Ibid* at para 12.

2. Hotel Rooms

There is a significant expectation of privacy in a hotel room.[116] Consistent with the Supreme Court of Canada's rejection of the "assumption of risk" doctrine, the fact that illicit activity is taking place in a hotel room does not diminish the occupants' expectation of privacy.

In *Wong*, the Court held that even though the accused invited members of the public to enter his hotel room to engage in illegal gambling, he continued to enjoy a reasonable expectation of privacy in the room's activities vis-à-vis the state.[117] Likewise, in *Mercer*, the Ontario Court of Appeal, applying *Wong*, excluded evidence of cannabis residue and cash that had been seized from the accused's hotel room despite the fact that the police were permitted to enter the room by hotel staff who had the right to enter the room.[118]

3. Personal Property

We enjoy a reasonable expectation of privacy in our personal effects and the information contained therein. Therefore, section 8 protects against warrantless searches of briefcases,[119] suitcases,[120] diaries,[121] cellphones,[122] and computers.[123]

Generally, to obtain the protection afforded by section 8 in one's personal property, one must be able to show a proprietary interest in the item.[124]

The situation is more complex when it comes to digital devices. After all, digital devices are private not because of anything about the plastic and silicon casing but because of the digital data stored on them. As discussed in greater detail below,[125] one may have a reasonable expectation of privacy in "sent" instant messages, texts, and emails residing on someone else's cellphone or computer,[126] or in data stored on a computer owned or controlled by someone else.[127]

116 *Wong*, *supra* note 17.
117 *Ibid.*
118 *Mercer*, *supra* note 49 at paras 10-15, 24-36.
119 *R v Mohamad*, 2004 CanLII 9378, [2004] OJ No 279 (QL) (CA).
120 *R v Chui*, [1996] AWLD 718 (Alta QB).
121 *R v Shearing*, 2002 SCC 58 at para 167.
122 *Fearon*, *supra* note 86.
123 *Morelli*, 2010 SCC 8 at paras 1-3.
124 *Edwards*, *supra* note 17 at para 44; *Belnavis*, [1997] 3 SCR 341 at para 24, 34 OR (3d) 806.
125 See Section VIII.C, "Informational Privacy."
126 *Marakah*, *supra* note 18 at para 4 ("depending on the totality of the circumstances, text messages that have been sent and received may in some cases be protected under s 8").
127 *Cole*, *supra* note 13.

4. Abandoned Items and Garbage

Where an item has been discarded or abandoned, the individual no longer enjoys an expectation of privacy in that item.[128] The question of whether an item has been abandoned depends on an objective assessment of the behaviour of the individual claiming the section 8 right.[129]

In *R v Patrick*, the police seized garbage bags adjacent to the accused's property but physically located in a public alleyway. The police did not have to step onto the accused's property but did have to reach through the airspace over Mr Patrick's property line. Applying the totality of the circumstances test from *Edwards*, the Court found that, when the accused's conduct was assessed objectively, he had abandoned his privacy interests in the garbage when he placed it at the rear of his property where it would be accessible to any member of the public including municipal garbage workers, or police pretending to be them.[130] Although the accused's territorial privacy interests were implicated by the intrusion over the property's airspace, that intrusion was "peripheral" and did not tip the balance under the totality of circumstances assessment.[131]

Courts have applied *Patrick* in the context of discarded DNA. In *R v Usereau*, the Quebec Court of Appeal held that the accused did not have a reasonable expectation of privacy in a glass and straw left at a restaurant.[132]

The fact that an item is stolen does not support an inference that the accused abandoned their expectation of privacy in the item. In *R v Law*,[133] the accused reported to the police that his safe had been stolen. A police officer recovered the safe but, suspecting the accused of tax fraud, forwarded the contents of the safe to Revenue Canada. The Supreme Court held that the accused retained a residual, albeit diminished, expectation of privacy in the contents of the stolen safe.

A distinction must be drawn between abandonment and simply leaving one's property unattended. Abandonment requires a wilful intent to discard one's property. Leaving one's property unattended does not. Thus, in *R v M(A)*, the majority held that the students did not abandon their privacy interests in their backpacks left unattended in the school gym.[134] As Binnie J wrote for the plurality: "My home is no less private when I am out than when I am there."[135] Similarly, where students leave

128 *Patrick*, *supra* note 18; *R v Krist*, 1995 CanLII 948, 100 CCC (3d) 58 (BCCA).
129 *Patrick*, *supra* note 18 at para 22.
130 *Ibid* at paras 55, 62.
131 *Ibid* at paras 38-41.
132 *Usereau*, 2010 QCCA 894, [2010] JQ No 4050 (QL).
133 *Law*, 2002 SCC 10.
134 *M(A)*, 2008 SCC 19 at para 48, Binnie J.
135 *Ibid* at para 48.

their closed backpacks in a room at school, they do not lose their privacy interests in the concealed contents.[136]

5. Airports and Border Crossings

The international border crossing is the paradigmatic example of privacy varying with context. In *R v Simmons*,[137] the Supreme Court held in 1988 that we enjoy a lower expectation of privacy at the border than in other contexts with respect to our person and our personal effects:

> I accept the proposition advanced by the Crown that the degree of personal privacy reasonably expected at customs is lower than in most other situations. People do not expect to be able to cross international borders free from scrutiny. It is commonly accepted that sovereign states have the right to control both who and what enters their boundaries.[138]

The Court in *Simmons* set up a sliding scale for personal privacy at the airport. A reasonable expectation of privacy at the border exists only in relation to highly invasive searches:

> First is the routine of questioning which every traveller undergoes at a port of entry, accompanied in some cases by a search of baggage and perhaps a pat or frisk of outer clothing. No stigma is attached to being one of the thousands of travellers who are daily routinely checked in that manner upon entry to Canada and no constitutional issues are raised. It would be absurd to suggest that a person in such circumstances is detained in a constitutional sense and therefore entitled to be advised of his or her right to counsel. The second type of border search is the strip or skin search of the nature of that to which the present appellant was subjected, conducted in a private room, after a secondary examination and with the permission of a customs officer in authority. The third and most highly intrusive type of search is that sometimes referred to as the body cavity search, in which customs officers have recourse to medical doctors, to X-rays, to emetics, and to other highly invasive means.[139]

Owing to security concerns, even on domestic flights one's reasonable expectation of privacy at the airport will be diminished. In *R v Lewis*, the Ontario Court of Appeal held that an accused's expectation of privacy was diminished because he was at the airport and intending to board a domestic flight.[140] As such, a warrantless search of his personal effects was not a violation of section 8 of the Charter.

136 *Ibid.*
137 [1988] 2 SCR 495 at 528-32, 67 OR (2d) 63.
138 *Ibid* at 528.
139 *Ibid* at 517.
140 *Lewis*, 1998 CanLII 7116, [1998] OJ No 376 (QL) (CA).

There is a broad statutory power under the *Customs Act*[141] to search items entering Canada. Section 99(1)(a) of the *Customs Act* provides that:

> 99(1) An officer may,
>
> (a) at any time up to the time of release, examine any goods that have been imported and open or cause to be opened any package or container of imported goods and take samples of imported goods in reasonable amounts

The Canadian Border Services Agency (CBSA) relies on the general search power in section 99(1)(a) of the *Customs Act* as authority for CBSA officers to conduct warrantless, groundless searches of any item entering Canada.

The CBSA has relied on this general search power as authority to conduct warrantless searches of travellers' cellphones. On this interpretation, the contents of a digital device are "goods." Under section 2(1) of the *Customs Act*, "goods" are defined to include "conveyances, animals and any document in any form." Further, "documents" includes electronic documents, and therefore, the CBSA has argued, border agents are authorized to search for electronic documents on travellers' digital devices.

Despite some obvious tension with more recent Supreme Court of Canada jurisprudence, which emphasizes the highly invasive nature of the search of one's cellphone,[142] the weight of authority at the trial level has accepted the Crown's interpretation of section 99(1)(a), and rejected section 8 Charter challenges.[143] The issue has not yet been addressed by the appellate courts.[144]

6. Common Carriers and Couriers

Though not as diminished as when travelling through an airport or an international border crossing, one's reasonable expectation of privacy is reduced when using a common carrier, such as a bus or train.[145] The Alberta Court of Appeal has held that the degree of the expectation of privacy in checked luggage on a common carrier is minimal.[146]

141 RSC 1985, c 1 (2nd Supp).

142 For commentary on this issue, see Nader Hasan and Stephen Aylward, "Cell Phone Searches at the Border: Privilege and the Portal Problem" (March 2017), 37:4 For the Defence 142; Robert J Currie, "Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?" (2016) 14 Canadian J of Law & Technology 289.

143 *R v Saikaley*, 2013 ONSC 1854; *R v Leask*, 2008 ONCJ 25; *R v Bares*, 2008 CanLII 9367 (Ont Sup Ct J); *R v Mozo*, 2010 CanLII 96558, [2010] NJ No 445 (QL) (NL Prov Ct); *R v Whittaker*, 2010 NBPC 32; *R v Moroz*, 2012 ONSC 5642.

144 The scope and interpretation of s 99(1) of the *Customs Act* was argued in *R v Saikaley*, 2017 ONCA 374, but the Court of Appeal did not address the issue.

145 *Kang-Brown*, *supra* note 2 at para 45, Binnie J, concurring.

146 *R v Matthiessen*, 1999 ABCA 31, 133 CCC (3d) 93.

7. Workplaces

There is an expectation of privacy in the workplace, albeit somewhat diminished.[147] To hold that no expectation of privacy exists in the workplace would create an unfairness for those of us for whom the workplace is a second home. As Blackman J remarked in *O'Connor v Ortega*:[148]

> It is, unfortunately, all too true that the workplace has become another home for most working Americans. Many employees spend the better part of their days and much of their evenings at work. … Consequently, an employee's private life must intersect with the workplace, for example, when the employee takes advantage of work or lunch breaks to make personal telephone calls, to attend to personal business, or to receive personal visitors in the office. As a result, the tidy distinctions (to which the plurality alludes, …) between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality.[149]

The reality of the modern workplace is that private, personal tasks must sometimes be completed at work. Those activities are entitled to a reasonable expectation of privacy. If an employee uses company stationery to write an intimate note to their spouse on company time, the company is not entitled to the information contained in that note. If an employee telephones their doctor from a company telephone, those communications do not belong to the company. Further, some employers are themselves "government" for the purposes of the Charter.

Generally, employees enjoy a reasonable expectation of privacy in the workplace vis-à-vis the state.[150] In determining the existence of the reasonable expectation of privacy and where it exists on the privacy spectrum, the court must consider both explicit workplace policies and rules as well as "operational realities" in determining the totality of the circumstances that inform the privacy equation.[151]

The Supreme Court has held that the *Hunter v Southam Inc* rules do not always apply to a government agency's inspectors' visit to the workplace for administrative or regulatory purposes given that there is a lower expectation of privacy and minimal intrusion in this context.[152]

147 *Silveira*, *supra* note 104; See *Thomson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 SCR 425, 72 OR (2d) 415; *Comité paritaire de l'industrie de la chemise v Potash*, [1994] 2 SCR 406, 168 NR 241.

148 *O'Connor v Ortega*, 480 US 709 (1987).

149 *Ibid* at 15.

150 *Silveira*, *supra* note 104 at 489; *Cole*, *supra* note 13.

151 *Cole*, *supra* note 13 at para 52.

152 *Comite paritaire de l'industrie de la chemise v Potash*, *supra* note 147 at paras 83-84; *Cole*, *supra* note 13.

8. Schools

Students enjoy a reasonable expectation of privacy at school. The level of privacy differs, however, depending on the context: students' expectations of privacy as against teachers and school officials will be lower than their expectation of privacy as against the police.[153]

In *R v M(MR)*,[154] the Supreme Court of Canada held that "the reasonable expectation of privacy of a student in attendance at a school is certainly less than it would be in other circumstances."[155] Although "weapons and drugs create problems that are grave and urgent," on the other side of the ledger is society's desire that "schools also have a duty to foster the respect of their students for the constitutional rights of all members of society":[156]

> Learning respect for those rights is essential to our democratic society and should be part of the education of all students. These values are best taught by example and may be undermined if the students' rights are ignored by those in authority.[157]

In *M(MR)*, the issue was the constitutionality of the frisk search ("turn out your pockets") of a student for drugs at a school dance by the vice-principal. The Court specifically held that if the search had been conducted by the police, or the school authorities acting as agents of the police, reasonable and probable grounds for belief would have been required. However, reasonable suspicion was sufficient for school authorities. The lesson of *M(MR)* is that in matters of school discipline, a broad measure of discretion and flexibility will be afforded the school authorities,[158] but when police are conducting a search, even on school premises, the ordinary standard of justification applicable to the police will be required.[159]

9. Temporary Lockers

It is not uncommon at stadiums, bus terminals, and amusement parks for the facility to rent out temporary storage lockers to the general public. The relationship between the user and the private entity operating the locker is governed by the contractual terms and conditions of the use of the locker as well as statutory privacy law. Nevertheless, even if the operator of the locker has a right of entry, this does not eliminate the user's reasonable expectation of privacy vis-à-vis the state.

---

153 *M(A)*, *supra* note 134 at paras 45-48.

154 [1998] 3 SCR 393, 233 NR 1; *R v Jarvis*, 2019 SCC 10, re students' privacy in the context of voyeurism.

155 *Ibid* at para 33.

156 *Ibid* at para 3.

157 *Ibid*.

158 *Ibid* at para 49.

159 *Ibid* at para 56; see also *M(A)*, *supra* note 134 at paras 45-48.

In *Buhay*, a private company owned the lockers at the bus terminal and could access even the locked lockers at any time.[160] Still, the Supreme Court held that the police could not justify their warrantless search of the accused's belongings from his rented bus depot locker simply because the private security guards who had contacted the police had earlier gone into the same locker with a master key and searched the same belongings. The accused's expectation of privacy was continuous. The intervention of the security guards at the bus depot did not extinguish that privacy interest or "relieve the police from the *Hunter v Southam Inc* requirement of prior judicial authorization before seizing contraband uncovered by security guards."[161]

10. Vehicles

We have a reasonable expectation of privacy in our personal vehicles, but that expectation of privacy is relatively lower than our reasonable expectation of privacy in our homes or personal offices.[162]

Because driving is an activity so highly regulated by the state, and because drivers are subject to a number of requirements, conditions, and regulations, a "reasonable level of surveillance of each and every motor vehicle is readily accepted, indeed demanded, by society … ."[163]

But even where police are authorized by law to conduct a check stop for some valid regulatory program, that power does not authorize the police to engage in a dragnet, pretextual search. Thus, in *R v Mellenthin*, where the police were lawfully authorized to conduct a motor vehicle check stop and shine a light into the vehicle, the subsequent search of a bag seen within the vehicle violated the accused's continued expectation of privacy.[164]

The reasonable expectation of privacy attaches to the person—not to the vehicle itself. Therefore, the section 8 claimant must show that they themself possess a reasonable expectation of privacy. Drivers will invariably have such an interest when they are in their own vehicles. Passengers may also have a reasonable expectation of privacy—depending on the circumstances. In *R v Belnavis*, a majority of the Supreme Court held that a passenger did not have a reasonable expectation of privacy in a car because she had no ownership over the car and no control over it.[165] The majority there distinguished the accused's circumstances with those of the spouse of the

160 *Buhay*, *supra* note 13 at paras 22-23.
161 *Ibid* at paras 22, 33-34, 38.
162 *Mellenthin*, [1992] 3 SCR 615, 144 NR 50; *Wise*, [1992] 1 SCR 527, 133 NR 161 [*Wise* cited to SCR].
163 *Wise*, *supra* note 162 at 534.
164 *Mellenthin*, *supra* note 162.
165 *Belnavis*, *supra* note 124 at para 19.

driver in a hypothetical case.[166] The Court also noted that passengers may possess a reasonable expectation of privacy in items within their control or that they owned.[167]

The current state of the law would appear to authorize dual purpose searches. In other words, even where the predominant purpose of the stop is to uncover illicit activity, such as drug trafficking, provided that the police also have a valid highway traffic regulatory purpose and can conduct their search in a manner that is specifically tailored to discovering evidence of driving offences, the search will not violate section 8 of the Charter. Thus, in *R v Nolet*, where the police officer randomly stopped a commercial vehicle to make inquiries authorized by provincial regulatory legislation, and conducted a search pursuant to that regulatory authority and discovered suspected proceeds of crime and marijuana, that search was deemed not to violate section 8 of the Charter.[168] The fact that the officer had all along suspected that the vehicle might be carrying drugs did not undermine the legitimacy of the search "[a]s long as there is a continuing regulatory purpose on which to ground the exercise of the regulatory power."[169]

More recent case law emphasizes that the holding in *Nolet* does not assist the police if any of their purposes were improper. Where racial profiling informs any part of the decision to search a vehicle or person, the police conduct will run afoul of section 9 of the Charter.[170] Thus, even if there are legitimate grounds to conduct a vehicle search, the search will be constitutionally infirm if the officer was motivated in any part by racial profiling.

11. Prisons

There is no iron curtain between the Charter and the prisons of this country.[171] Prisoners continue to enjoy Charter rights, including section 8 rights, albeit in a more limited form.[172] Thus, a prisoner does not have a reasonable expectation of privacy with respect to their location within a prison.[173] Nor does a prisoner have a reasonable expectation of privacy with respect to searches of their person, despite the nearly inviolate protection of bodily integrity outside of the prison context.[174] Nor does a prisoner have an expectation of privacy with respect to personal documents on their person[175] (other than, of course, material protected by solicitor–client privilege).

166 *Ibid* at para 23.
167 *Ibid* at para 24.
168 *Nolet*, 2010 SCC 24 at paras 39-43.
169 *Ibid* at para 41.
170 *R v Dudhi*, 2019 ONCA 665 at paras 55-66.
171 See *Wolff v McDonnell*, 418 US 539, 555-556 (1974), White J ("[t]here is no iron curtain drawn between the Constitution and the prisons of this country").
172 *R v Major* (2004), 188 OAC 159, 186 CCC (3d) 513 (CA).
173 *R v Dorfer* (1996), 104 CCC (3d) 528, 69 BCAC 197 (CA).
174 *R v Garcia*, 1992 CanLII 3917, 72 CCC (3d) 240 (Qc CA).
175 *R v Lamirande*, 2002 MBCA 41, 164 CCC (3d) 299.

12. Shared Areas and Overlapping Privacy

To obtain the protection of section 8 of the Charter, the applicant must show that the state has invaded their *own* expectation of privacy (as opposed to that of a third party). In *R v Edwards*, the accused failed to establish that he had a reasonable expectation of privacy in his girlfriend's residence.[176] Applying the *Edwards* factors, the Supreme Court held that there were insufficient objective indicia militating in favour of a reasonable expectation of privacy: the accused stayed at the apartment infrequently, he did not contribute to rent, and he had no authority to admit or exclude others.[177] Although "[c]ourts applying *Edwards* have … typically rejected s. 8 claims made by visitors, landlords, former residents, and even occupants' children,"[178] it is important to bear in mind that *Edwards* does not create a bright line test for the "shared home" context, but rather, a flexible rule. Each case will turn on the individual *Edwards* factors.

The Supreme Court of Canada's decision in *Reeves*,[179] though not dealing directly with physical spaces, ought to be read alongside *Edwards* and its progeny. Indeed, Karakatsanis J's majority opinion appears to make it clear that the Court in *Reeves* was not just writing for the personal computer context, but with respect to overlapping privacy interests at large:

> [A]lthough the privacy interests of co-occupants or co-users over some shared premises or items may be "overlapping," it does not follow that those interests are "coextensive." Indeed, where the consent giver and the claimant are not the same person, the s. 8 *Charter* inquiry does not concern the legitimacy of the former's privacy interests in the subject matter of the search or seizure, but rather the latter's expectation of privacy in it.[180]

The emphasis here on "co-occupants" and "shared premises" alongside "co-users" and "shared items" suggests that Karakatsanis J was writing beyond the facts of this case. *Reeves* should be considered binding authority when addressing any overlapping privacy issue. Although Karakatsanis J explicitly declined to decide whether the police could lawfully enter the common areas of a shared residence with the consent of one resident, fact patterns analogous to *Edwards* should now be approached with caution.[181] *Reeves* has arguably superseded *Edwards* at least in part.

The earlier cases applying *Edwards* must also be read with an eye towards more recent case law dealing with the related issues of common areas in apartment buildings

176 *Edwards*, *supra* note 17 at paras 47-50.
177 *Ibid*.
178 See Steven Penney, Vincenzo Rondinelli & James Stribopoulos, *Criminal Procedure in Canada* (Toronto: LexisNexis, 2011) at 157 (collecting cases).
179 *Reeves*, *supra* note 20.
180 *Ibid* at para 53.
181 See *R v Yu*, 2019 ONCA 942 at paras 70-74 (for discussion on reasonable expectation of privacy in shared physical spaces).

and condominiums. In *R v White*, the Ontario Court of Appeal held that the accused had a reasonable expectation of privacy in the common areas of his condominium building.[182] Despite the numerous lower court decisions rejecting claims of reasonable expectation of privacy in the common areas of multi-unit buildings, the *White* Court held that the *Edwards* factors tugged in a different direction here: "the lesson from *Edwards* is that the reasonable expectation of privacy is a context-specific concept that is not amenable to categorical answers."[183] In *White*, the relatively small size of the building, the fact that the accused owned his unit, and the assumption that the building security systems would keep out intruders, augured in favour of finding a reasonable expectation of privacy.[184]

Subsequent trial court decisions attempted to distinguish *White* on its facts and suggested that one *generally* does not have a reasonable expectation of privacy in the common areas of multi-dwelling-unit buildings.[185]

The Ontario Court of Appeal has rejected this narrow approach. In *R v Yu*, the Ontario Court of Appeal held that there was a sliding scale of privacy in a condominium building. In that case, the accused did not have a reasonable expectation of privacy in the parking garages, but did have a diminished expectation of privacy in their hallways.[186] While the only time that condominium residents should expect complete privacy "is when they are inside their unit with the door closed,"[187] there is a diminished but reasonable expectation of privacy in various of the common areas:

> Once inside an access-controlled condominium building, residents are entitled to expect a degree of privacy greater than what, for instance, they would expect when approaching the building from the outside. This results from the fact that anyone can view the building from the outside, but there is some level of control over who enters the building.
>
> The level of expectation of privacy inside a condominium building will vary. The level of expectation of privacy is dependent on the likelihood that someone might enter a certain area of the building, and whether a person might reasonably expect a certain area to be subject to camera surveillance.
>
> Some areas of condominium buildings are routinely accessed by all condominium residents, such as the parking garage or elevator lobby. The level of expectation of privacy in those areas is low, albeit remaining greater than would be expected outside of the building. The level of expectation of privacy increases the closer the area comes to a person's residence, such as the end of a particular hallway of a particular floor of the building.

182 *White*, 2015 ONCA 508. See contra *R v Laurin*, 1997 CanLII 775, 113 CCC (3d) 519 (Ont CA); *R v Thomsen*, 2007 ONCA 878.

183 *White*, *supra* note 182 at para 44.

184 *Ibid* at paras 45-48.

185 *R v Brewster*, 2016 ONSC 8038 at para 62, reversed by *Yu*, *supra* note 181, leave to appeal to SCC refused, [2020] SCCA No 38 (QL); *R v Zekarias*, 2018 ONSC 4752 at para 19.

186 *Yu*, *supra* note 181 at para 69.

187 *Ibid* at para 86.

> Even in those less-frequented areas the level of expectation of privacy is low, but not as low as in the more commonly used areas.[188]

As to whether the reasonable expectation of privacy of the condominium-dweller extends to an expectation that their movements will not be captured on video, that expectation will depend on whether the cameras are visible, and whether the resident has been informed by the condominium management as to the location of any security cameras installed in the building: "If there is no visible camera, and if the resident has been told that there are no security cameras, then residents are entitled to expect their movements are not subject to camera surveillance."[189]

13. Public Spaces

State agents are free to observe us as we walk down public streets, en route to our homes, offices, places of worship, or anywhere else we may choose to spend our time. The state's unaided observation of people does not infringe a reasonable expectation of privacy.[190]

While public spaces are, by definition, not private ones, we do maintain an interest in anonymity as we go about our daily lives. Being spotted by strangers and neighbours as we move about our daily business is entirely different from having the state watch and record our every move. Privacy, as a constitutionally protected interest, entails a reasonable expectation of anonymity.

Anonymity permits individuals to act in public places but to preserve freedom from identification and surveillance.[191] The fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of their privacy rights, despite the fact that as a practical matter, such a person may not be able to control who observes them in public. Thus, in order to uphold the protection of privacy rights in some contexts, we must recognize anonymity as one conception of privacy.[192]

In *Wise*, the Supreme Court of Canada held that the ubiquitous monitoring of a vehicle's whereabouts on public highways amounted to a violation of the suspect's reasonable expectation of privacy.[193] The Crown argued that the electronic device was simply a convenient way of keeping track of where the suspect was driving his

188 *Ibid* at paras 82-84.

189 *Ibid* at para 85.

190 See *Wise*, *supra* note 162 (drawing a distinction between unaided surveillance in public and electronic surveillance of a person's whereabouts in public).

191 *Spencer*, *supra* note 54 at para 43; see A Slane and LM Austin, "What's In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" (2011) 57 Crim LQ 486 at 501.

192 *Spencer*, *supra* note 54 at para 44, citing E Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50:3 UTLJ 305 at 325-26.

193 *Wise*, *supra* note 162.

car, something that he was doing in public for all to see, but the Court rejected such an approach. There was a reasonable expectation of privacy. Admittedly, the Court in *Wise* found that the invasion of privacy was "minimal," but such a finding stemmed both from the fact that driving is a heavily regulated activity and that the device at issue was technologically very rudimentary.

The Supreme Court has not directly revisited *Wise* in a more technologically advanced context, but its decision in *Spencer* is instructive.[194] *Spencer* did not address anonymity in the physical world, but rather, anonymity in a virtual world. In *Spencer*, the issue was whether there could be privacy or anonymity in our movements around the Internet—a quintessentially public space.

In *Spencer*, the police were able to use publicly available tools to identify the IP address associated with a user who was sharing child pornography. The subscriber information (name, telephone number, and address) associated with that IP address was not publicly available but was within the knowledge of that user's ISP.[195] The Crown took the position that no production order was required to compel the ISP to produce the subscriber information. After all, there is nothing private about someone's name and address.

The Supreme Court disagreed. What was being sought was not simply generic biographical information; "it was the identity of an Internet subscriber which corresponded to particular Internet usage."[196] Knowing both the IP address, and associated user activity, combined with identifying information, would tell you a great deal about that individual's biographical core. Browsing logs, website "cookies," and other records, reveal a significant amount about a user's interests, concerns and habits. Browsing the Internet involves navigating a public space but in a largely anonymous way. Because the subscriber information was the key to unlocking a treasure trove of revealing information about the Internet user, the accused did have a reasonable expectation of privacy in the identifying information.[197]

In *Spencer*, the Supreme Court cited *Wise* with approval for the proposition that section 8 protects privacy as anonymity in public spaces.[198] The broad language of *Spencer*, and its reliance on *Wise*, makes it persuasive, if not binding, authority for questions involving surveillance or tracking, regardless of whether the issue involves the real or the virtual world.

194 *Spencer*, *supra* note 54.
195 *Ibid* at paras 7-12.
196 *Ibid* at para 32.
197 *Ibid* at para 45.
198 *Spencer*, *supra* note 54 at paras 43-44.

C. Informational Privacy

Informational privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[199] The Supreme Court of Canada has endorsed a robust approach to "informational self-determination."[200] This right recognizes that "all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit."[201]

The Supreme Court of Canada has taken a purposive approach to informational privacy. The subject matter must not be defined "narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action."[202]

Thus, when it comes to informational privacy, the courts draw a distinction between the information to which a reasonable expectation of privacy attaches and the physical device or storage unit housing that information. As a result, the ownership or control over the physical device is not necessarily determinative of the privacy rights: "control is not an absolute indicator of a reasonable expectation of privacy, nor is lack of control fatal to a privacy interest."[203] Indeed, on numerous occasions, the Supreme Court has recognized a reasonable expectation of privacy in places and things that are not exclusively under the claimant's control.[204]

1. Informational Privacy and the Biographical Core

The closer that information lies to an individual's "biographical core," the more likely it is to be protected under section 8 of the Charter.

As Sopinka J explained in *R v Plant*:[205]

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from

199 *Tessling*, *supra* note 3 at para 23, quoting AF Westin, *Privacy and Freedom* (New York: Atheneum, 1970) at 7.

200 *Jones*, *supra* note 11 at para 39.

201 *Ibid* at para 39; *Dyment*, *supra* note 16 at 429; *Spencer*, *supra* note 54 at para 40.

202 *Reeves*, *supra* note 20 at para 29; *Marakah*, *supra* note 18 at para 15, citing *Vancouver (City) v Ward*, *supra* note 71 at para 65. The guiding question is "what the police were really after" (*Marakah*, *supra* note 18 at para 15, citing *Vancouver (City) v Ward*, *supra* note 71 at para 67).

203 *Marakah*, *supra* note 18 at para 38; *Reeves*, *supra* note 20 at para 37.

204 *Marakah*, *supra* note 18 at paras 38-45; *Jones*, *supra* note 11; *Buhay*, *supra* note 13 at paras 22-23; *Cole*, *supra* note 13 at paras 50-54 and 58; also *Marakah*, *supra* note 18 at paras 38-45; *Edwards*, *supra* note 17 at para 45(6)(iii).

205 [1993] 3 SCR 281, 157 NR 321.

> dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[206]

And as Justice Fish wrote in *Cole*:[207]

> The closer the subject matter of the alleged search lies to the biographical core of personal information, the more this factor will favour a reasonable expectation of privacy. Put another way, the more personal and confidential the information, the more willing reasonable and informed Canadians will be to recognize the existence of a constitutionally protected privacy interest.[208]

This is not to suggest that section 8 protects personal information *only* where that information lies at the biographical core. Even where the information at issue does not lie at the biographical core, other factors may still tip the scales in favour of finding a reasonable expectation of privacy. Indeed, the Ontario Court of Appeal affirmed that section 8 can "protect informational privacy interests beyond that 'biographical core.' "[209]

The reasonable expectation of privacy exists on a spectrum. One can have a high expectation of privacy, a "diminished expectation of privacy," or no privacy at all.[210] Where the information at issue does not lie at the biographical core, then subject to the other factors in the *Edwards* analysis, the individual may have a diminished expectation of privacy. Where the reasonable expectation of privacy lies on the spectrum may inform the section 8 analysis, and will almost certainly inform the exclusion analysis under section 24(2) of the Charter in the event that the court finds a section 8 breach.[211]

2. The Reasonable Expectation of Privacy in Data Stored on Digital Devices

It is now trite law that one enjoys a high expectation of privacy in one's personal digital device. Given "the personal nature of the material on the [computer], a subjective expectation of privacy can be presumed."[212] The personal nature of the information

206 *Ibid* at 293.
207 *Cole*, *supra* note 13.
208 *Ibid* at para 46.
209 See *Orlandis-Habsburgo*, 2017 ONCA 649 at para 79. See also *M(A)*, *supra* note 134 at paras 67-68.
210 *Orlandis-Habsburgo*, *supra* note 209 at para 111 ("[a] reasonable though diminished expectation of privacy is nonetheless a reasonable expectation of privacy, protected by s 8 of the Charter").
211 See e.g. *Cole*, *supra* note 13 at para 92 (where the Supreme Court found a reasonable expectation of privacy in a workplace computer and a s 8 violation, but did not exclude the evidence because the expectation of privacy was "diminished").
212 *R v Little*, 2009 CanLII 41212, [2009] OJ No 3278 (QL) at para 126 (Sup Ct J); See also *Cole*, *supra* note 13 at para 43.

on the computer also makes that expectation objectively reasonable. That expectation of privacy is further augmented by the unique ways in which computers work and store data.

Although computers and computer-generated data have been vital sources of evidence in criminal and civil cases for decades, section 8 of the Charter was a late arrival to the digital age. The birth of the constitutional right to digital privacy originates with the Supreme Court of Canada's decision in *R v Morelli*.[213]

3. Personal Computers and Digital Devices

In *Morelli*,[214] the Court, seemingly for the first time, turned its mind to the highly intrusive nature of a search of one's personal computer. A computer technician had arrived at the accused's house to install a high-speed Internet connection. He noticed, among other things, Internet links to adult and child pornography in the browser taskbar's favourites list. The technician contacted a social worker, who informed the RCMP. The RCMP subsequently obtained a warrant to enter the accused's home and search his computer. The ensuing search revealed evidence of child pornography. The Supreme Court held that the search violated section 8 of the Charter. The warrant should not have been issued because statements contained in the Information to Obtain (ITO) were misleading and erroneous.

The most important part of the judgment is the Court's analysis under section 24(2) of the Charter. The Court excluded the improperly obtained evidence under section 24(2) because of the highly invasive nature of a search of the accused's personal computer. Justice Fish wrote:

> It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer.
>
> First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created. The police scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet—generally by design, but sometimes by accident. …
>
> Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.

213 *Supra* note 123.
214 *Ibid.*

> It is therefore difficult to conceive a s. 8 breach with a greater impact on the *Charter*-protected privacy interests of the accused than occurred in this case.[215]

This holding animates all of the Supreme Court of Canada's subsequent decisions on digital privacy. Justice Fish does not merely describe a personal computer search as "highly invasive." Instead, it is "difficult to imagine a search *more* intrusive, extensive or invasive of one's privacy."[216]

Justice Fish also shows insight into the unique nature of the information on or available to the computer. It is not just that the computer is a repository of vast amounts of private information that, in an earlier time, would have been locked away in a desk drawer or a filing cabinet. The computer also stores information from which the state can recreate an "electronic roadmap" of one's "cybernetic peregrinations,"[217] including one's Internet search history, which is a powerful window into one's innermost thoughts and curiosities.

The invasiveness of searching a computer or other digital device is a function of the profound privacy interests residing in one's computer data. As the Supreme Court held in *Cole*:[218]

> Computers that are used for personal purposes, regardless of where they are found or to whom they belong, "contain the details of our financial, medical, and personal situations" (*Morelli*, at para. 105). This is particularly the case where, as here, the computer is used to browse the Web. Internet-connected devices "reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet" (*ibid.*).
>
> This sort of private information falls at the very heart of the "biographical core" protected by s. 8 of the *Charter*.[219]

The Supreme Court of Canada elaborated on these concepts in *R v Vu*.[220] A high expectation of privacy attaches to information stored on a computer or smartphone in part because of the nature of the information stored on the computer but also due to other unique features of the computer that make computer searches particularly invasive.

First, the *quantity* of the information stored on computers is unlike anything in the physical world.[221] For less than $100, anyone can purchase a computer hard drive

215 *Ibid* at paras 2-3, 105-6.
216 *Ibid* at para 2 (emphasis added).
217 *Ibid* at para 3.
218 *Cole*, *supra* note 13.
219 *Ibid* at paras 47-48.
220 2013 SCC 60.
221 *Ibid* at para 24 ("[c]omputers potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search").

with storage capacity of 1 terabyte (1000 GB), which is roughly equivalent to 500 million pages of text—or about the amount of information contained in all of the books on 12 floors of an academic library.[222] Given this "massive storage capacity," the Supreme Court noted, there is a significant difference between the search of a computer and the search of a briefcase or filing cabinet found in the same location.[223]

Second, the type of information stored on a computer is often intimate and private, thereby "fall[ing] at the very heart of the 'biographical core' protected by s. 8 of the *Charter*." [224] Virtually every aspect of one's private life is consolidated into one's computer, including "our most intimate correspondence," "details of our financial, medical, and personal situations," and "our specific interests, likes, and propensities" as revealed through the records of what we "seek out and read, watch, or listen to on the Internet."[225] People today use computers as photo albums, stereos, telephones, desktops, filing cabinets, waste paper baskets, televisions, postal services, playgrounds, jukeboxes, dating services, movie theatres, shopping malls, personal secretaries, virtual diaries, and more.[226] Your computer may reveal to the world more about you than your spouse, family members, or close friends ever could.

Third, the computer is a "fastidious record keeper."[227] Computers contain information that is automatically generated, often unbeknownst to the user. This computer-generated "metadata" tracks information about who created a document on what date or who visited a given website at a particular time. It can reveal significant private information about the user's interests, habits, and identity.[228]

Fourth, a computer retains files and data even after users think they have destroyed them.[229] When a user "deletes" a file, the operating system simply marks the disk clusters occupied by that particular file as available for future use by other files. If the operating system does not reuse that cluster for another file by the time the computer

222 Orin S Kerr, "Searches and Seizures in a Digital World" (2006) 119 Harv L Rev 531 at 542; see also Marc Palumbo, "How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment" (2009) 36:5 Fordham Urb LJ 977 at 995.

223 *Vu*, *supra* note 220 at para 41.

224 *Ibid* at para 40; *Cole*, *supra* note 13 at para 48.

225 *Morelli*, *supra* note 123 at paras 3, 105; *Cole*, *supra* note 13 at para 47.

226 Kerr, "Searches and Seizures in a Digital World," *supra* note 222 at 569. See also Lesley Taylor, "The Astonishing Amount of Personal Data Police Can Extract from Your Smartphone," *Toronto Star* (28 February 2013), online: <www.thestar.com/news/world/2013/02/27/the_astonishing_amount_of_personal_data_police_can_extract_from_your_smartphone.print.html> (where a police search of a smartphone revealed 104 call logs; eight passwords; 422 text messages; six wireless networks; and 10,149 files of audio, pictures, text, and videos—378 of which were deleted).

227 *Vu*, *supra* note 220 at para 42.

228 *Ibid*.

229 *Ibid* at para 43.

is searched, the file marked for deletion will be available for forensic examination.[230] Even if another file has been assigned to that cluster, a large amount of that data can be forensically recovered from the computer's "slack space"—that is, space within the cluster left temporarily unused.[231] In an era where hard drive data storage now exceeds multiple terabytes, this means that many of us unwittingly retain massive amounts of data we attempted to delete. Your computer's "delete" key thus is more appropriately described as the "hide" button—it hides files from the casual user but not from the future forensic examiner.

Finally, a computer is rarely a stand-alone, self-contained entity. A computer that is connected to a network or to the Internet is a portal to a world exponentially larger than the computer itself.[232] A search of a computer that the police have lawful authority to access could give police access to other users' information stored on other devices and for which the police have no lawful authority to search.

These unique factors "call for distinctive treatment under s. 8 of the *Charter*,"[233] and ought to inform any reasonable expectation of privacy analysis when dealing with digital devices and digital data.

4. The Biographical Core and the Internet of Things

The digital age also greatly complicates the idea of the "biographical core." As noted above, the types of information stored on a computer—personal correspondence, family photographs, banking records, Internet activity—lie at the biographical core.

But counsel and the courts should be cautious to avoid a narrow approach to the question of whether data lies at the biographical core. The "biographical core" of digital data is a matter of some complexity, owing again to the unique features of digital devices and digital technologies.

There is no doubt that a journal entry or personal communication traditionally falls within the "biographical core." So too would personal banking or medical records. This is not new. Such information was private in an earlier era; it remains in the digital age when such information is stored on a digital device.

The digital age also introduced a range of new categories of information that people did not generate during an earlier time. For example, using the Internet will generate an "Internet search history"—a trail of bread crumbs of all of your "cybernetic

230 Edward TM Garland & Donald F Samuel, "The Fourth Amendment and Computers: Is a Computer Just Another Container or Are New Rules Required to Reflect New Technologies?" (2009) 14:5 Ga BJ 14 at 16; Kerr, "Searches and Seizures in a Digital World," *supra* note 222 at 542; *Little*, *supra* note 212 at para 96.

231 *Vu*, *supra* note 220 at para 43, citing *Kerr*, "Searches and Seizures in a Digital World," *supra* note 222 at 542.

232 *Ibid* at para 44.

233 *Ibid* at para 45.

peregrinations"[234] around the Internet, tracking everywhere you have visited and on what days.

Using a digital device creates so-called "metadata." Metadata is machine-generated data that is a byproduct of using the device. Metadata is data about data. For each user-generated file, such as a word-processing document, a spreadsheet, or a photograph, your digital device encodes into the file all kinds of information about the *who*, *what*, *where*, *when*, and *how* each bit of information was created. Your selfie in front of the Eiffel Tower may be entirely innocuous in itself, but the metadata embedded in the image file that pinpoints your location in Paris on a specific date, at a specific time, might prove to be highly probative in a police investigation. Depending on the context, metadata can be as revealing—or even more revealing—about your biographical core than the content of the user-generated document, video, or image.

Other information that may at first blush appear mundane and outside of the biographical core may be profoundly revealing when situated in context with other data points. For example, there is nothing private about one's name or address—facts that are found in the phone book or its modern equivalent, such as <https://411.ca>. But that so-called "tombstone" information can be intensely revealing when coupled with other information, such as one's Internet search history. This was the key lesson of the Supreme Court of Canada's decision in *Spencer*, in which the Court held that Internet subscribers have a reasonable expectation of privacy in their basic subscriber information.

In *Spencer*, an officer of the Saskatoon Police Service was engaged in a child pornography investigation. Using the publicly available Limewire file-sharing software, the officer searched for users sharing child pornography. Limewire also permitted him to see the IP addresses associated with each user. He ran a list of IP addresses against a database with approximate locations and found that one of the IP addresses had an approximate location of Saskatoon, with Shaw Communications Inc as the ISP.[235]

The police, however, did not know where the computer with that IP address was located. The officer then made a request to Shaw under section 7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act*,[236] requesting the subscriber information associated with the IP address. No warrant was obtained. Shaw complied with the request and provided their customer's name, address, and telephone number.

The question on appeal was whether section 8 demands that a warrant be sought and obtained to access Internet subscriber information. The Crown argued that section 8 protects informational privacy only where the user has a reasonable expectation of privacy. In *Morelli* and *Cole*, the data searched involved information going to the accused's core biographical information. In *Spencer*, however, the information

234 *Morelli*, *supra* note 123 at para 3.
235 *Spencer*, *supra* note 54 at paras 7-12.
236 SC 2000, c 5.

sought—the name, address, and telephone number matching a publicly available IP address—did "not touch on the core of Mr. Spencer's biographical information."[237] There is no privacy in a name and address.

The Supreme Court disagreed. What was being sought was not simply generic biographical information—"it was the identity of an Internet subscriber which corresponded to particular Internet usage."[238] Knowing both the IP address and associated user activity, combined with identifying information, would tell you a great deal about that individual's biographic core. Accordingly, the accused did have a reasonable expectation of privacy in the identifying information.[239]

Said differently, while the IP address was publicly visible to other online users, and there is nothing inherently private about your name and address, it is the connecting of the dots that is revelatory. The IP address, coupled with Internet activity associated with that IP address, in combination with the name and address of the IP address user, is intensely revealing of one's biographical core.

Spencer's significance has only grown since the emergence of the "Internet of Things." The Internet of Things refers to the ability of everyday objects to connect to the Internet and send and receive data.[240] It refers to the countless connections between our phones, computers, and all of our "smart" devices. It includes, for example, Internet-connected cameras, home automation systems (e.g., smart security cameras, smart fridges, smart dryers), smart watches and "Fitbits," smart energy meters, smart health care devices (providing real-time updates to healthcare providers), and smart cars.

The Internet of Things means that courts and counsel will increasingly have to consider the ways in which different data sets *in combination* with other data sets affect privacy rights. Any single data set or data point—such as the readings from your smart fridge or your smart car—in isolation might not be particularly revealing. But when matched with these other data sets, and then in combination with your name and address, they can be intensely revealing. The data generated from the Internet of Things is in many ways like a Georges Seurat pointillist painting. If you look at it up close, it's just a series of dots. But take a step back and it evokes a vivid image of an individual's private life.[241] The collection of certain individual data points might not be a privacy violation, but at some point, enough individual data points, collected and analyzed together, will give rise to a reasonable expectation of privacy.

---

237 *Spencer*, *supra* note 54 at para 25.

238 *Ibid* at para 32.

239 *Ibid* at para 45.

240 US Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World* (January 2015).

241 This approach implicates what some American scholars call the "Mosaic Theory" of privacy. See Orin S Kerr, "The Mosaic Theory of the Fourth Amendment" (2012) 111:3 Mich Law Rev 311.

The holding in *Spencer* has already prompted the appellate courts to revisit old precedents. In *Plant*, and then again in *R v Gomboc*, the Supreme Court refused to recognize a reasonable expectation of privacy in energy consumption records because those records did not go to the biographical core of personal, intimate details of the lifestyle and personal choices of the appellants.[242]

Yet, in *R v Orlandis-Habsburgo*,[243] another decision dealing with whether an accused had a reasonable expectation of privacy in energy consumption records, the Ontario Court of Appeal declined to follow *Plant* or *Gomboc*. Instead, it applied the more recent decision in *Spencer* (which was about Internet subscriber data, not energy consumption). Justice Doherty, on behalf of a unanimous panel, wrote:

> With the benefit of the analysis in *Spencer*, I am satisfied that the appellants had a reasonable expectation of privacy in their energy consumption data. The examination and use of that data without the appellants' consent constituted a "search" and "seizure" under s. 8 of the *Charter*.[244]

Electricity records in isolation might not go to the biographical core. But when situated alongside other information, they might be intensely revealing.

5. Electronic Communications

One may continue to enjoy a reasonable expectation in electronically delivered text messages or emails, including messages that reside on third parties' phones and over which you no longer exercise effective control. This was the key holding of *Marakah*[245] and *Jones*,[246] two companion cases decided by the Supreme Court of Canada in 2017.

In *Marakah*, the accused sent incriminating text messages to his accomplice. The police searched the accomplice's phone and sought to introduce the incriminating text messages against Mr Marakah. At issue in *Marakah* was whether the accused had a reasonable expectation of privacy in messages *sent* by the accused but *stored on* the accomplice's phone. The accused had no property interest in the accomplice's phone, nor any control over how the accomplice used his phone or to whom he forwarded the accused's messages. Still, the majority held that in the totality of the circumstances, the accused retained a reasonable expectation of privacy in the sent text messages.[247]

Like in *Marakah*, the accused in *Jones* had sent electronic messages to an accomplice, Mr Waldron. Unlike in *Marakah*, the police in *Jones* used a third-party production order to obtain account information and data from Mr Waldron's carrier, Telus.

242 *Plant*, *supra* note 205; *Gomboc*, 2010 SCC 55 at para 50.
243 *Supra* note 209.
244 *Ibid* at para 115.
245 *Marakah*, *supra* note 18.
246 *Supra* note 66.
247 *Marakah*, *supra* note 18.

The question was whether *Jones* had standing to challenge that production order on section 8 grounds. The Court held that he did.

This was not like the case where someone has discarded garbage (which suggests a meaningful choice to abandon one's privacy).[248] And although Mr Jones, like Mr Marakah, lacked physical control over the messages, that factor is not dispositive. The Court concluded that, "as a normative matter, it is reasonable to expect a service provider to keep information private where its receipt and retention of such information is incidental to its role of delivering private communications to the intended recipient."[249]

6. Internet Chat Rooms and Public Message Boards

Marakah and *Jones* will have wide-ranging implications for all kinds of electronic and Internet-based communications. They left open the question of whether one has a reasonable expectation of privacy—diminished or not—in a public or quasi-public Internet forum like a chat group or Facebook message board.

The Supreme Court of Canada addressed this issue in the child-luring context in *R v Mills*.[250] In *Mills*, a police officer posed online as a 14-year-old girl with the intent of catching Internet child-lurers. Using Facebook and Hotmail, the accused sent the undercover officer sexually explicit messages and arranged a meeting in a park, where he was arrested and charged with child-luring. Without having obtained prior judicial authorization, the officer used screen-capture software to create a record of his online communications with the accused. The accused applied for the exclusion of the evidence on the ground that this was a warrantless search and thus a section 8 violation.

A plurality of the Court held that section 8 was not engaged *on facts of this case* because adults cannot reasonably expect privacy online with children whom they do not know. Indeed, the plurality acknowledged the modesty of its holding: "that Mills cannot establish an objectively reasonable expectation of privacy in these particular circumstances, where he conversed with *a child* online who was *a stranger* to him and, *most importantly*, where the police knew this when they created her."[251]

The plurality left for another day whether the answer might be different in an adult–adult online conversation. The plurality also left open—and indeed explicitly contemplated a different result—if the police had been monitoring Internet chat rooms "in the hope of stumbling upon a conversation that reveals criminality."[252]

248 See e.g. *Patrick*, *supra* note 18; *Stillman*, *supra* note 89.
249 *Marakah*, *supra* note 18 at para 44.
250 2019 SCC 22.
251 *Ibid* at para 30 (emphasis in original).
252 *Ibid.*

7. Shared Computers

One user of a shared computer cannot waive another user's reasonable expectation of privacy: "By choosing to share a computer with others, people do not relinquish their right to be protected from the unreasonable seizure of it."[253] Thus, in *Reeves*, the Supreme Court of Canada held that one spouse's consent to the police's seizure of the shared computer did not extinguish the other spouse's reasonable expectation of privacy in the information contained on the computer. The Court found a section 8 violation and excluded the evidence found thereon.[254] Writing for the majority, Karakatsanis J held:

> I cannot accept that, by choosing to share our computers with friends and family, we are required to give up our *Charter* protection from state interference in our private lives. We are not required to accept that our friends and family can unilaterally authorize police to take things that we share. The decision to share with others does not come at such a high price in a free and democratic society.[255]

The Supreme Court's decision in *Reeves* follows a line of Supreme Court of Canada cases that hold that ownership and control, though relevant, are not determinative of privacy rights.[256]

In *Cole*, the accused, a high school teacher, was permitted to use his work-issued and school board–owned laptop for incidental personal purposes. He browsed the Internet and stored personal information on his hard drive. When a school technician found a hidden folder containing nude photographs of a female student on the accused's computer, he notified the principal. The principal copied the photographs onto a CD and seized the laptop, both of which were handed over to the police, who, without a warrant, reviewed their contents and created a mirror image of the hard drive for forensic purposes. The accused did not own the computer hardware but he did own the personal and private information stored on it—private information that "falls at the very heart of the 'biographical core' protected by s. 8 of the *Charter*."[257] Accordingly, the Supreme Court held that the accused had a reasonable expectation of privacy in his work-issued computer, and that the warrantless search of the computer had violated section 8.

253 *Reeves*, *supra* note 20 at para 37.
254 *Ibid* at para 61.
255 *Ibid* at para 44.
256 *Buhay*, *supra* note 13 at paras 22-23; *Cole*, *supra* note 13 at para 54; *Marakah*, *supra* note 18 at paras 38-45; *Edwards*, *supra* note 17 at para 45(6)(iii). See also *Cole*, *supra* note 13 at para 48.
257 *Cole*, *supra* note 13 at para 48.

8. Electricity Records and Thermal Energy Readings

Owing to cannabis growers' need for abundant and irregular amounts of electricity, there is a rich jurisprudence on search and seizure in relation to electricity consumption records. But as our understanding of privacy in the modern age has evolved, so too has the case law in this area.

In *Plant*, the police obtained electricity consumption records from a utility showing the total energy consumed at a residence for a six-month period.[258] The Supreme Court declined to find that the residents had a reasonable expectation of privacy in the records because the data provided very little information about the lifestyle or activities of the occupants. This result was driven by the fact that the information at issue fell outside the "biographical core" of information in need of protection in a free and democratic society.[259]

In *Gomboc*,[260] the Supreme Court of Canada revisited the issue 17 years later. The digital recording ammeter (DRA) readings at issue in *Gomboc* used more sophisticated technology and gave more detailed readings than the records at issue in *Plant*. Yet, the plurality focused on the fact that the DRA data still did not reveal much about the biographical core of the residents and thus held that the residents did not have a reasonable expectation of privacy in the DRA readings.[261]

Tessling deals with different technology but similar issues.[262] In *Tessling*, the RCMP used an airplane equipped with a FLIR camera to overfly properties owned by the accused. FLIR technology records images of thermal energy or heat radiating from a building. It could not, at this stage of its development, determine the nature of the source of heat within the building or "see" through the external surfaces of a building. Accordingly, the Court declined to find a reasonable expectation of privacy in relation to the FLIR readings, but noted that future advances in technology rendering the FLIR cameras more invasive might be grounds for revisiting that holding.[263]

In *Orlandis-Habsburgo*, another decision dealing with whether an accused had a reasonable expectation of privacy in energy consumption records, the Ontario Court of Appeal took a different approach. Justice Doherty, on behalf of a unanimous panel, noted that even though information that lay closer to the biographical was more likely to fall within the ambit of a reasonable expectation of privacy, that fact alone was not dispositive.[264] In other words, section 8 protects more than just information that lies at the biographic core of the individual.[265] Justice Doherty took the position that the

258 *Plant*, *supra* note 205.
259 *Ibid* at 293.
260 *Gomboc*, *supra* note 242.
261 *Ibid* at paras 39, 81.
262 *Tessling*, *supra* note 3.
263 *Ibid* at para 58.
264 *Orlandis-Habsburgo*, *supra* note 209.
265 *Ibid* at para 79. See also *M(A)*, *supra* note 134 at paras 67-68.

Supreme Court's more recent decision in *Spencer* (which was about Internet subscriber data, not energy consumption) superseded *Plant* and *Gomboc*, and held on the basis of *Spencer* that the appellants had a reasonable expectation of privacy in their energy consumption data.[266]

9. Olfactory Searches

In the companion cases of *R v Kang-Brown*[267] and *M(A)*,[268] the Supreme Court of Canada held that the use of police dogs to detect the odour of illegal drugs emanating from personal property encroaches upon a reasonable expectation of privacy. A dog's "sniff" thus constitutes a "search" for section 8 purposes. The dog sniff may reveal information relating to the biographical core of information protected by section 8, including intimate and private details of a person's lifestyle and personal choices.[269]

10. Airline Manifests

In *R v Chehil*, on-duty RCMP officers at an airport attended at the airline office to view a passenger manifest for an arriving domestic flight. Based on information that the accused paid cash for a one-way ticket purchased shortly before departure, the officers formed suspicion that he was a drug courier. The accused was charged with possession of cocaine for purpose of trafficking after a police dog indicated the presence of narcotics in his bag. Mr Chehil argued that the warrantless search of the airline manifest violated his section 8 rights. The trial judge granted the application and excluded the evidence.[270] The Nova Scotia Court of Appeal, however, reversed.[271] It held that the information at issue "did not reveal intimate details of his lifestyle or personal choices and was not specific and meaningful information intended to be private and concealed."[272] Nor did the information at issue provide a direct link to information that lay at the biographical core.[273]

11. Documents, Records, and Fillable Forms

Unsurprisingly, one has a reasonable expectation of privacy in one's private business, banking, and medical records.[274] In *Schreiber v Canada (AG)*,[275] the Court held that it

266 *Orlandis-Habsburgo*, *supra* note 209.
267 *Kang-Brown*, *supra* note 2.
268 *M(A)*, *supra* note 134.
269 *Supra* note 2 at para 58.
270 *Chehil*, 2008 NSSC 357.
271 *R v Chehil*, 2009 NSCA 111, aff'd 2013 SCC 49.
272 *Ibid* at para 57.
273 *Ibid* at para 56.
274 *R v Jarvis*, 2002 SCC 73 at paras 95-98 (reasonable expectation of privacy in financial documents).
275 [1998] 1 SCR 841, 158 DLR (4th) 577.

was clear that the "personal financial records" at issue in that case, which had been obtained from a bank, fell within the "biographical core" protected by section 8 of the Charter.[276]

What happens when we disclose sensitive or private business, banking, medical, or other information to third parties? In the modern regulatory state, we are often asked by both state agencies and private companies to complete forms disclosing private information. In determining whether an individual has a reasonable expectation of privacy in information disclosed in a form, it is important to consider the purpose for which the information was disclosed.[277] Consistent with the Supreme Court's rejection of the "third-party doctrine," the fact that you voluntarily surrender your confidential information to a third party such as a bank does not mean that you have voluntarily surrendered your privacy interest vis-à-vis the state. That said, even within the banking context where there is an inherent privacy interest, the information must be of a confidential and personal nature to attract a reasonable expectation of privacy.[278]

There may be a diminished expectation of privacy in documents, business, and tax records kept pursuant to regulatory schemes. Even there, however, the law distinguishes between different branches of the state. Where tax records are kept pursuant to a valid regulatory scheme, one may have a substantially reduced reasonable expectation of privacy vis-à-vis the Canada Revenue Agency, but one may retain an ongoing residual expectation of privacy vis-à-vis the police.[279]

IX. Conclusion

In the 21st century, one's reasonable expectation of privacy is increasingly a function of the interplay between technology and law. From IMSI catchers to the "Internet of Things," technology enables law enforcement to intrude upon individual privacy in ways never even imagined only a few years ago. In years past, physical and technological limits made mass surveillance prohibitively expensive, if not impossible, for law enforcement. Today, it is no longer possible for the individual to pull the drawbridge up.[280] If there are to be meaningful limits on the state's ability to intrude upon individual privacy, those limits will be imposed by law.

276 *Ibid* at para 22.
277 *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403, 132 FTR 55.
278 See e.g. *R v Lillico*, 1994 CanLII 7548, 92 CCC (3d) 90 (Ont Gen Div).
279 *Jarvis*, *supra* note 274 at paras 72, 84-99.
280 *Tessling*, *supra* note 3 at para 16.