1 Reasonable Expectation of Privacy in Digital Data

I. Introduction

A search or seizure occurs when police action intrudes on a "reasonable expectation of privacy."[1] A reasonable expectation of privacy includes both a subjective and an objective component. It is a finding based on the totality of circumstances and a key battleground of litigation in the digital era; absent a reasonable expectation of privacy, an accused does not have standing to challenge a search or seizure.

Totality of circumstance is a broad umbrella. The mass of digital information potentially available relating to any given person is vast. Every bank transaction, email, wi-fi connection, purchase, membership, job, hobby, friend, and event may be captured in some digital form or another. It is no surprise, then, that the inquiry into what is expected and what is objectively reasonable in modern society is a challenging one. Ownership, access, and control—all concepts traditionally applied in privacy analysis—have different meanings in a digital world of connectivity and anonymity. These concepts have evolved through careful consideration by Canadian courts to adapt to new understandings of what we want, hope, and expect to keep from state eyes.

This chapter explores the basics of defining a privacy interest in digital data and the application of those concepts to different types of information (e.g., subscriber information versus content) and different contexts, such as home and office computers, the border, online activity, and sent communications. For counsel working in this area, the significance of the determination of a reasonable expectation of privacy cannot be overstated. It opens or ends the *Canadian Charter of Rights and Freedoms*[2] section 8 analysis. Lawyers and judges alike need to understand the first principles of privacy to effectively consider appropriate extensions or restrictions on those principles and the attendant rights and state obligations in digital contexts.

II. Defining Privacy

Privacy may be physical, territorial, informational, or some combination of the three. Digital evidence most commonly engages concerns over informational privacy, although occasionally other interests can overlap. Courts sometimes comment on territorial concerns where, for example, a computer is used or found in a bedroom or a workplace, but given the mobility of technology and the accessibility of digital data from multiple locations, the spatial boundaries to privacy are increasingly meaningless. Particularly after the COVID-19 pandemic, a bedroom tablet may be a mobile phone and a platform for office videoconferencing. Files created in a home setting may be intended for and broadcast immediately to a worldwide audience. Individuals' expectations of privacy in digital data relate less to where they use devices and more to what

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

2 Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [Charter].

they use them for. Practically, this means that arguments should focus less on *where* the device is stored, found, or used and more on *what* information the state is accessing.

Traditional privacy analysis focused largely on the tangible factors of control and access to locations where evidence was seized. In *R v Edwards*, the Supreme Court of Canada (SCC) set out a flexible framework with key questions to ask in assessing privacy interests.[3] The non-exhaustive list of factors identified as instructive for the privacy analysis in *Edwards* is as follows:

(i) presence [of the accused] at the time of the search;
(ii) possession or control of the property or place searched;
(iii) ownership of the property or place;
(iv) historical use of the property or item;
(v) the ability to regulate access, including the right to admit or exclude others from the place;
(vi) the existence of a subjective expectation of privacy; and
(vii) the objective reasonableness of the expectation.[4]

Edwards dealt with a claim of privacy over evidence found in an apartment that the accused did not own. However, despite the territorial privacy at issue in that case, the *Edwards* framework remains relevant and has been adapted to a modern context and to claims of informational privacy.[5]

Several modifications of the "totality of the circumstances" test have been articulated to organize the analysis in a given fact scenario. For example, in *R v Patrick*,[6] a case involving garbage bags put out for collection and retrieved by police, Binnie J listed factors similar to those in *Edwards* but geared toward addressing situations where territorial and information privacy overlap:

1. What was the nature or subject matter of the evidence gathered by the police?
2. Did the accused have a direct interest in the contents?
3. Did the accused have a subjective expectation of privacy in the informational content of the evidence?
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 accused's property and, if so, what is the impact of such a finding on the privacy analysis?

3 *R v Edwards*, 1996 CanLII 255 at para 45 (SCC).

4 *Ibid*.

5 See e.g. *R v Plant*, [1993] 3 SCR 281 at 303-4, 1993 CanLII 70; *R v Tessling*, 2004 SCC 67 at para 32; *R v Cole*, 2012 SCC 53 at paras 39-58; *R v Patrick*, 2009 SCC 17 at para 27.

6 *Patrick*, *ibid* at para 27.

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 accused's lifestyle, or information of a biographic nature.

R v Spencer[7] similarly refined the analysis, this time in a case dealing with informational privacy relating to Internet service subscriber data in the hands of third-party companies. In that case, Cromwell J, for the Court, organized the expectation of privacy analysis into four general areas: (1) the subject matter of the alleged search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances.[8] None of these tests is inconsistent; they are articulations of the same overarching concerns grouped differently as suited to a particular inquiry. Again, the argument on *what* data were seized, not on *where* the machine sat at seizure or during use, is the best focus.

The *Spencer* formulation has served as a versatile framework for privacy assessments in a diverse range of digital evidence cases, such as for considering IP addresses (*R v Bykovets*[9]), text messages (*R v Marakah*,[10] *R v Campbell*[11]), energy consumption data (*R v Orlandis-Habsburgo*[12]), and event data recorders in vehicles (*R v Attard*[13]).

Although the focus is appropriately on what data has been seized, the reasonable expectation of privacy inquiry has historically—and importantly—been content neutral.[14] This means that the fruits of a search cannot be used after the fact to justify an unreasonable privacy violation.[15] The fact that an accused may be engaged in criminal

7 2014 SCC 43.
8 *Ibid* at para 18.
9 2024 SCC 6.
10 2017 SCC 59.
11 2024 SCC 42.
12 2017 ONCA 649.
13 2024 ONCA 616.
14 *Campbell*, *supra* note 11 at paras 50-52.
15 *Marakah*, *supra* note 10 at para 48.

behaviour does not direct the reasonable expectation of privacy analysis. The SCC has repeatedly emphasized that

> [t]he nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. The analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought.[16]

A primary factor to consider under any privacy rubric is the nature of the information obtained and the extent to which it falls within the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."[17] This factor can often be determinative of the analysis. Courts adopt a broad and purposive approach in defining the subject matter of a privacy claim. Defence counsel push as much as they can into that core, and Crown counsel try to narrowly restrict it. It is worthwhile for counsel to spend time properly characterizing the digital evidence at issue.

In *R v Plant*, the SCC first defined the protected zone of privacy as encompassing information touching on a biographical core. The Court held that electricity consumption records held by electrical utility companies did not fall within the biographical core; while they revealed the pattern of electricity consumption in the residence, they did not reveal any intimate details of personal lifestyle or private decisions.[18] Thus, section 8 of the Charter did not apply to the access that police gained to a computer terminal, the utility set up to allow police to look up the appellant's electrical consumption records.

In *R v Gomboc*, however, information of a similar nature had a different hue.[19] Six out of nine judges of the SCC in *Gomboc* found that the installation of a digital recording ammeter (DRA) on the appellant's power line by the utility company (at the request of the police) engaged the "biographical core" of personal information belonging to the appellant (although seven of nine judges ultimately held that the appellant did not have a reasonable expectation of privacy as a result of other factors in the totality of the circumstances). The difference between the DRA in *Gomboc* and the electricity records in *Plant* is that the former revealed electricity consumption patterns at a much higher level of detail, allowing stronger inferences to be drawn about the precise household activities giving rise to those consumption patterns (e.g., marijuana grow operation).

16 *Spencer*, *supra* note 7 at para 36.

17 *Plant*, *supra* note 5 at 293.

18 *Ibid*.

19 *R v Gomboc*, 2010 SCC 55 at para 38, Deschamps J; at para 81, Abella J; and at paras 128-32, McLachlin CJ and Fish J, dissenting.

The strength of the inference supported by the information is critical.[20] Crown counsel would want to argue that electrical consumption never changes—it is not core data. But defence counsel may find traction, as in *Gomboc* and *Orlandis-Habsburgo*, in arguing that the data reveals more about the target than a metric output. The more defence counsel can tie the data obtained to intimate lifestyle choices and features, the more likely a court is to see it as falling under the biographical core umbrella and worthy of section 8 protection.

The definition of the scope of information obtained by police is a key factor in determining the outcome of a reasonable expectation of privacy inquiry. The narrower the scope and the further the information from the core, the less likely a privacy right will be established (although note that s 8 of the Charter can protect informational privacy interests beyond the biographical core).[21]

The importance of defining the subject matter of the search was reinforced in *Spencer*.[22] There, the SCC considered whether individuals have a reasonable expectation of privacy in their Internet customer name and address, which their Internet service provider (ISP) could connect with a particular Internet Protocol (IP) address at a given point and time in cyberspace. The Crown emphasized the limited nature of the specific information at issue (the name and address), while the defence emphasized what the information could reveal once combined with an IP address (the individual's online activities).[23] The Court was persuaded by the latter view and focused its analysis on the strength of the inference that the targeted information could support. An individual's name and address, once combined with the IP address, could identify the individual with "intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous."[24] It was therefore reasonable to expect that this information would remain private. A law enforcement request for such information from the ISP was found to be a search within the meaning of section 8.[25] Thus, *Spencer* demonstrates the importance of persuading the court on the proper characterization of the information at stake in litigation concerning whether there is a reasonable expectation of privacy.[26] That said, the subject matter of a search should not "take on hypothetical dimensions" and must remain "rooted in reality."[27] In *R v El-Azrak*,[28] the Court of Appeal for Ontario therefore held that

20 See discussion of *Gomboc* by the Court in *Spencer*, *supra* note 7 at para 30.

21 *Ibid*; *R v AM*, 2008 SCC 19 at paras 67-68.

22 *Supra* note 7.

23 *Ibid* at para 24.

24 *Ibid* at para 66.

25 *Ibid*.

26 See also *Bykovets*, *supra* note 9, discussed later in this chapter.

27 *R v El-Azrak*, 2023 ONCA 440 at para 40.

28 *Ibid*.

the data obtained from a Drug Usage Report from a pharmacy (which included the dates on which fentanyl was prescribed, the prescription number, and the strength and quantity of the fentanyl dispensed) was not sufficiently private to militate toward finding a reasonable expectation of privacy in that data. The Court held that the subject matter of a search cannot be "retroactively characterized according to what the information reveals after it has been combined with other investigative facts."[29] If that was the case, virtually all information the police obtained could ultimately result in privacy claims.[30] The private nature of the subject of a search would also constantly be in flux, frustrating the police's ability to discern whether prior judicial authorization is required.[31]

Beyond defining the nature of the information, the courts must also consider whether the individual has a subjective expectation of privacy in the information and whether that expectation of privacy is objectively reasonable. The threshold for establishing a subjective expectation of privacy is relatively modest and will typically be established in most cases.[32] That said, there are limits. For example, in *R v Sidhu*, the Alberta Court of King's Bench held that an accused did not have a subjective expectation of privacy in a CCTV recording of a VIP room in a nightclub.[33]

A subjective expectation may be inferred from the circumstances in the absence of the accused's testimony, or the accused may simply rely on the Crown's theory of the prosecution.[34] If the Crown alleges that the accused is the author of specific incriminating text messages, for example, the accused may rely on that allegation to establish a subjective expectation of privacy on a section 8 claim without having to take the stand and offer direct evidence of authorship.[35] This prevents the accused from having to take on the "dangerous gambit" of testifying on a *voir dire* to establish the basis for a section 8 Charter claim when that testimony could be contrary to what the accused's substantive position would be on the trial proper.[36]

29 *Ibid* at para 48.

30 *Ibid*.

31 *Ibid* at paras 49-52.

32 *R v Jones*, 2017 SCC 60 at paras 19-20.

33 *R v Sidhu*, 2024 ABKB 56 at paras 34-36. See also *R v Budlakoti*, [2020] OJ No 6058 (QL) at paras 87-89 (SC), where the Ontario Superior Court held that the applicant did not have a subjective expectation of privacy in text messages exchanged with a police agent given the applicant's obvious concerns about the messages attracting police attention.

34 *Jones*, *supra* note 32 at para 21. Note that before *Jones*, it was unclear whether the defence could rely on the Crown's theory of the case in support of an argument that an accused had a subjective expectation of privacy. Cases decided before *Jones* regarding this issue should, therefore, be approached with caution.

35 *Ibid* at para 9.

36 *Ibid* at para 22.

The most difficult part of the section 8 analysis is the question of whether the expectation of privacy is objectively reasonable. This is a thorny area of shifting parameters and much debate. The reasonable expectation of privacy under section 8 is one that changes over time to reflect social values and modern civilized expectation, awareness, and objectives. Privacy is a normative concept. It must be considered anew in each setting and case. Courts assessing privacy interests must consider not only what we actually believe is confidential or protected, but also the nature of the information we *want* to keep private.[37] The social values of Canadian society weigh heavily in the mix. Social values will, of course, change and conflict.

Modern social values include not only a deep concern for private information but also a seemingly unprecedented drive for publicity through sharing every minute detail of life in public online forums. Particularly in the younger generation, selfies abound and social media is a virtual smorgasbord of bite-sized reports on every imaginable human experience. In *Tessling*, Binnie J, for the Court, remarked that "a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place."[38] Yet we do not relinquish control over every intimate detail we may have to impart in digital form when we file taxes, book a medical appointment, transfer funds, or share messages with a partner.

Consider, for example, recent litigation regarding pole camera surveillance. In *R v Hoang*,[39] the Court of Appeal for Ontario held that although pole camera surveillance *may* give rise to an objective expectation of privacy in appropriate circumstances—considering, for example, the duration, scope, and nature of the surveillance; the reason for its placement; or its location—that was not the case for the pole surveillance in *Hoang*. There, police mounted a pole camera outside the accused's house, in public, and recorded the movement of people and vehicles into and out of the home over a nine-day period. The Court of Appeal held that the trial judge had not erred in concluding that Mr Hoang did not have an objectively reasonable expectation of privacy in the public space in front of the house that the pole camera captured or, alternatively, that any expectation of privacy he did have was "highly diminished."[40]

In the public spaces of online activity, the line is unclear.[41] Albeit in a different context, consider the SCC's comments in *R v JJ* regarding the constitutionality of the

37 *Spencer*, *supra* note 7 at para 18; *Tessling*, *supra* note 5 at para 42; *Patrick*, *supra* note 5 at para 14.

38 *Tessling*, *supra* note 5 at para 40.

39 2024 ONCA 361, leave to appeal to SCC dismissed, 2024 CanLII 90807 (SCC).

40 *Ibid* at paras 46-47. See also *Papenbrock-Ryan v Vancouver (City)*, 2024 BCSC 2288 at paras 126-38; *R v Moore*, 2023 ONCJ 98 at paras 105-14. But see *R v Aubrey*, 2022 ONSC 635 at paras 30-51, where the Court agreed with the accused that police installation of video surveillance of his private residence was a "flagrant and egregious breach" of his s 8 rights because the camera had a better vantage point of the residence than was available to the naked eye.

41 *R v Craig*, 2016 BCCA 154 at para 48.

section 278.92 "defence records" regime.[42] A complainant in a sexual offence case must have a reasonable expectation of privacy in a piece of evidence for it to engage *Criminal Code*,[43] section 278.92 screening. Answering that question requires courts to assess the *context* in which the evidence was created, part of which involves considering *where* the material was shared. To that end, the Court stated that

> records created or obtained in the public domain, where they could be accessed by multiple people or the general public (e.g., social media or news media), are less likely to attract a reasonable expectation of privacy. That said, the fact that certain information is already available somewhere in the public sphere does not preclude further harm to the privacy interest through additional dissemination that would increase access to the information.[44]

In other words, even if a complainant discloses personal information publicly online, this does not necessarily preclude an argument that the same information should not be disseminated in court. Although the Court's record screening analysis is not directly transferable to the section 8 context, the Court's comments may nevertheless be instructive when considering the growing societal tension between the competing desires for privacy and publicity.

The SCC elaborated on a modern legal conception of privacy in *Spencer*, defining informational privacy as comprised of three elements: secrecy, control, and anonymity.[45] The inclusion of anonymity as one of the three key components of privacy was somewhat new ground, though certainly, discussion of anonymity as a feature of privacy interests was not novel. In stressing the importance of anonymity in the online context, the Court drew on the Court of Appeal for Ontario decision in *R v Ward*. In *Ward*, Doherty JA identified a significant personal interest in operating free from state surveillance in our daily lives. He explained:

> Personal privacy is about more than secrecy and confidentiality. Privacy is about being left alone by the state and not being liable to be called to account for anything and everything one does, says or thinks. Personal privacy protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society.[46]

42 *R v JJ*, 2022 SCC 28.

43 RSC 1985, c C-46.

44 *JJ*, *supra* note 42 at para 60.

45 *Spencer*, *supra* note 7 at para 38.

46 *R v Ward*, 2012 ONCA 660 at para 71; see also paras 72-74.

The application to the Internet context and the suggestion of a right to anonymity in the online world is an extension of uncertain ambit. The *Spencer* Court acknowledged the concern that the overextension of online anonymity protection could impede the investigation of Internet crime, but responded that recognizing that privacy interests may exist (depending on the circumstances) does not create a *right* to online anonymity and need not impede law enforcement's effectiveness. As Cromwell J explained:

> In my view, recognizing that there *may* be a privacy interest in anonymity depending on the circumstances falls short of recognizing any "right" to anonymity and does not threaten the effectiveness of law enforcement in relation to offences committed on the Internet. In this case, for example, it seems clear that the police had ample information to obtain a production order requiring Shaw to release the subscriber information corresponding to the IP address they had obtained.[47]

This flexible approach makes good sense given the tension between the right to be left alone by the state and the strong societal interest in, for example, undercover police operations targeting anonymous online criminal behaviour.

The SCC considered the factor of control in the cases of *Cole*[48] and *Marakah*.[49] *Cole* dealt with the search of a workplace computer used by the individual Charter claimant but owned by the individual's employer (who had access to the computer's contents for specific purposes). *Marakah* dealt with text communications sent by the individual to another person. In both instances, the individual claimant did not have exclusive control over the subject of the search. Nonetheless, in both instances, the SCC recognized a reasonable expectation of privacy.

Marakah in particular recognized that control is "not an absolute indicator of a reasonable expectation of privacy, nor is lack of control fatal to a privacy interest."[50] Rather, it is merely one factor, and it must be viewed in the context of the subject matter of the search. In the case of text communications, for example, the act of giving up a degree of control over the information is inherent in the exercise of engaging in a conversation. The individual is still exercising a measure of control over the information by deciding how, when, and to whom they disclose that information.[51] Just because they choose to give up control vis-à-vis the recipient of the text communication does not mean that they should be treated as having given up control of the information vis-à-vis the state. To argue that they have is to fall into the error of engaging in "risk analysis" (i.e., the notion that an individual abandons their expectation of

47 *Spencer*, *supra* note 7 at para 49 (emphasis in original).

48 *Supra* note 5.

49 *Supra* note 10.

50 *Ibid* at para 38; *Cole*, *supra* note 5 at paras 54, 58.

51 *Marakah*, *supra* note 10 at para 39.

privacy when they create the risk that their information will fall into the hands of the state).[52] That is not how a normative analysis under section 8 of the Charter works. Privacy is relational; disclosure to one is not disclosure to all.[53]

Ultimately, the reasonable expectation of privacy analysis requires an examination of the totality of circumstances. Although this approach facilitates flexible and contextual decision-making for courts assessing state conduct after an event has transpired, the nuanced and rapidly changing digital landscape can create challenges for law enforcement required to make dynamic front-line decisions about the scope of their powers. Continuing education for officers in this area is therefore critical to maintaining the integrity of their investigations.

It is helpful that classes of digital information have emerged from the case law as ones in which particular factors weigh more heavily than others. The existence of a reasonable expectation of privacy, however, remains a case-specific determination. Reasonable expectation of privacy in digital evidence may vary depending on where the data are stored, who has access, who has control, how the state can obtain it, and what the information reveals or may inferentially reveal. Some trends are discernable in the manner in which courts approach different types of digital evidence.

III. Expectation of Privacy in Subscriber Information and IP Addresses

Subscriber information is basic information about a person who enters a contract for telecommunications, Internet, or other services. In the context of digital evidence, subscriber information usually includes the customer's name, municipal address, billing information, and account details obtained from a service provider. The kind of service at issue and the basis of the police request for information will influence whether and what kind of judicial authorization is required for the state to access subscriber information.

In *Spencer*,[54] the SCC found a reasonable expectation of privacy in subscriber information related to Internet activity. The facts were fairly straightforward. Police had identified an IP address associated with the transmission of child sexual abuse material through a publicly available Internet file-sharing platform. They were able to determine—again, through a publicly available online source—which ISP was responsible for the targeted IP address. In order to link the alleged child sexual abuse material transmission to a particular suspect, police requested basic subscriber information from the ISP associated with the IP address during the relevant time period. There was no judicial pre-authorization. The ISP responded to the request and provided a name, a municipal address, and basic account details. Police obtained a search warrant for the

52 *Ibid* at para 41.

53 See also Nader Hasan et al, *Search and Seizure* (Toronto: Emond, 2021) ch 2 at s VI.

54 *Supra* note 7.

address, where they located a computer belonging to the accused, who was not the service subscriber, that contained child sexual abuse material.

The SCC found a breach of section 8 in the police acquisition of subscriber details relating to Internet activity. Instrumental in determining the reasonable expectation of privacy was a broad definition of the subject matter of the search. While it was argued that a customer name and address was not the kind of core biographical information that could support a section 8 claim, the Court looked beyond the "tombstone data" and considered what that information could reveal when combined with other information already known to police. The Court was concerned with linking online activity that was carried out anonymously with known identifiers. Given the vast scope of activity potentially pursued online, the solid link to a personal identity was considered significant enough to require constitutional protection.

The *Spencer* Court defined the subject matter of the search in a contextual fashion. *Spencer* cannot be taken to require prior judicial authorization for all kinds of tombstone customer data. It is the online activity link that raised the expectation of privacy. For now, telephone subscriber data do not engage the same concerns, though, no doubt, counsel in some future case will find the platform to argue that the phone now acts as an Internet search portal and is thus entitled to the same privacy considerations. In *R v Ahmad*, for example, a majority of the SCC described a phone number as providing "access to an intensively private virtual space" allowing people to "cultivate personal, work and family relationships through [their] phones; they are a portal of immediate access reserved for the select few closest to us."[55] While the Court made these comments in the context of entrapment, one can easily imagine the same observations grounding a section 8 analysis. Digital evidence contexts will always require fact-specific analysis of the totality of circumstances.

A significant development in this sphere came in *Bykovets*, where the SCC held that IP addresses—unique numbers assigned to electronic devices by ISPs—attract a reasonable expectation of privacy.[56] Moving forward, the police therefore now require prior judicial authorization to obtain IP address information. The case involved a police investigation into fraudulent online purchases from a liquor store. A third-party payment processing company, Moneris, managed online sales. The police contacted Moneris directly to obtain the IP addresses related to specific purchases, and Moneris volunteered two IP addresses belonging to the accused and his father. The IP addresses led to the discovery of incriminating evidence, including credit data, credit card writing equipment, fraudulent documents, and firearms. The SCC held that although IP addresses do not, on their own, reveal personal biographical

55 *R v Ahmad*, 2020 SCC 11 at para 36. See also *R v Boutros*, 2018 ONCA 375 at paras 30, 36; *R v Baskaran*, 2020 ONCA 25 at paras 45-47. But see *El-Azrak*, *supra* note 27 at para 88, where the Court of Appeal for Ontario held that "standing on its own, a cellular phone number does not engage with the lifestyle and personal choices of the accused."

56 *Bykovets*, *supra* note 9.

information, they are "the key to unlocking a user's Internet activity and, ultimately, their identity";[57] the first "digital breadcrumbs" to establishing a user's "entire daily, weekly, or even monthly online activity, leading to an electronic roadmap of the user's cybernetic peregrinations."[58] Ultimately, an IP address has the potential to betray intensely private information that touches on the most "intimate details of the lifestyle and personal choices of an individual user."[59]

The SCC's decision in *Bykovets* will have immediate implications for police conducting child sexual abuse material investigations.[60] Law enforcement in countries around the world use a "Child Protection System" (CPS)—a software program that combs peer-to-peer networks to identify suspected child sexual abuse material and log the IP address and global unique identifier (GUID, an alphanumeric code that is generated when peer-to-peer software is downloaded to a computer associated to the child sexual abuse material). Before *Bykovets*, courts had held that there is no reasonable expectation of privacy in a GUID, which is "exactly like an IP address" in the sense that it reveals nothing about a particular individual.[61] Post-*Bykovets*, cases in this area should be approached with caution. Law enforcement agencies would be wise to review their policies and practices for compliance; otherwise, defence counsel may seize on the opportunity to argue that the use of CPS was unlawful, particularly for investigations conducted after *Bykovets* when the police no longer have the benefit of being able to rely on the law as it stood at the time of the investigation for the purposes of a section 24(2) analysis.

The impact of *Bykovets* in child sexual abuse investigations is already apparent. In *R v Daniels*,[62] the Ontario Superior Court held that the police violated the accused's reasonable expectation of privacy by using an IP address contained in a report from the National Center for Missing and Exploited Children (NCMEC, an organization in the United States that receives reports from Internet companies that become aware of child sexual abuse material or child exploitation on their systems). In *Daniels*, the police used the IP address to obtain a production order for subscriber information. The Court found that this was a section 8 violation because the IP address was used as a link to specific user activity.

Unlike online activity, which is often anonymous, telephone conduct has historically been more limited in scope and not anonymous, given the public listing of

57 *Ibid* at para 28.

58 *Ibid* at para 69.

59 *Ibid* at para 70.

60 See Wes Dutcher-Walls & Jocelyn Rempel, "Search Solutions and Techno Tricks—Early Thoughts on Bykovets in P2P Investigations and Mandatory Reporting" (2024) 44:3 For the Defence 38.

61 *R v Nguyen*, 2017 ONSC 1341 at paras 35-47. See also *R v El-Halfawi*, 2021 ONCJ 462 at paras 81-94.

62 2025 ONSC 344.

most numbers and addresses in virtual, if not paper, phonebooks. For example, the Ontario Superior Court held that not all customer name and address information attracts a reasonable expectation of privacy.[63] In *TELUS*, police had obtained a transmission data recorder warrant (TDRW) under section 492.2 of the *Criminal Code*.[64] TDRWs authorize the police to prospectively obtain *transmission data* about a target from third-party telecommunications companies. Transmission data are data about telecommunications (i.e., metadata) but do not include the contents of the communications or the name and address of the customer participating in the communications. To bridge the latter evidentiary gap, police sought an assistance order under section 487.02 of the *Criminal Code* to compel Telus to reveal the customer name and address of the cellphone in question.

The issue was whether individuals have a reasonable expectation of privacy in this information such that a separate judicial authorization was required, as an assistance order is not a standalone search power. Nordheimer J said no. He distinguished *Spencer* on the basis that the customer name and address information in *Spencer* led police to a trove of information, while the customer name and address in this case was just that and nothing more.[65] Again, the analysis turned on the strength of the inference that the information could support. Where the customer name and address did not open the door to a new world of revealing information, Nordheimer J held that there was no reasonable expectation of privacy.[66]

The decision in *TELUS* was followed by the Court of Appeal of Newfoundland and Labrador in *Reference re: Criminal Code (Can) s 487.02*.[67] There, the Court held that an assistance order is available to require telecommunication companies to provide subscriber information associated with a telephone number captured by the lawful use of a TDRW. In so holding, the Court noted that while section 492.2 explicitly excludes content from the definition of transmission data, it does not explicitly exclude subscriber data:

> [T]he fact that obtaining subscriber information is not precluded by section 492.2 is an indication that Parliament did not intend to prevent police from requiring telcos to produce it and that Parliament expected or assumed that it could be lawfully obtainable by means of an assistance order.[68]

63 *HMQ v TELUS Communications Company*, 2015 ONSC 3964 at para 24.

64 The TDRW is one of the many new search powers introduced by the *Protecting Canadians from Online Crime Act*, SC 2014, c 31, discussed in detail in Chapter 3.

65 *Spencer*, *supra* note 7 at para 40.

66 *Ibid* at para 30. For a summary of the pre-*Spencer* case law on customer name and address associated with a phone number, see Code J's decision in *R v Khan*, 2014 ONSC 5664.

67 2019 NLCA 6, leave to appeal to the SCC refused, 2019 CanLII 99450 (SCC).

68 *Ibid* at para 56.

Without subscriber information, the raw data produced by the TDRW is largely meaningless.[69]

In *TELUS*, Nordheimer J was careful to also distinguish cases concerning cellphone records, which reveal not just the customer name and address but actual metadata concerning the calls, such as the times and durations of calls, as well as the telephone numbers for calls made and received.[70] The courts have long held that there is a reasonable expectation of privacy in this information, including in *R v Rogers Communications*.[71]

Privacy is a normative concept that will always be subject to fresh analysis. Social values and practices change, law enforcement capabilities develop, technology advances, and formerly innocuous or unavailable bits of information become more significant and potentially more revealing. No categorical statements can be made about what type of subscriber information or digital identifiers will continue or begin to attract a reasonable expectation of privacy. Defence counsel seeking to establish a reasonable expectation of privacy in information obtained by police should give serious thought to the type of evidence they can adduce at trial to establish the social values and practices that will bolster their argument. This may be done by way of an expert or expert report. For example, in *Bykovets*, defence filed a forensic investigator's report summarizing the functions of IP addresses, but a formal expert may not be necessary. Social science literature, privacy commission reports, and polls or surveys on the use of new technological tools or apps are just a few examples of the types of evidence that may prove invaluable in shaping the section 8 debate—particularly as cases move up the appellate ladder. Any materials submitted should be capable of being tested in court, and courts should be cautious about improperly taking judicial notice of contentious facts.

IV. Expectation of Privacy in Computers and Electronic Devices

Devices vary, as do privacy interests engaged in police searches or seizures thereof. On the very high end of the scale, police examination of a personal computer was found in *R v Morelli* to be the most intrusive state search imaginable.[72] In the oft-quoted introduction to the majority decision in *Morelli*, Fish J described the scale of privacy interest in a home computer search:

69 The Court of Appeal for Ontario declined to decide whether subscriber information relating to a telephone number engages a reasonable expectation of privacy: *R v Khan*, 2023 ONCA 361 at para 10.

70 *TELUS*, *supra* note 63 at para 37.

71 2016 ONSC 70 at para 31. See also *R v MacInnis*, 2007 CanLII 29342 (ONSC); *R v Mahmood*, 2008 CanLII 51774 (ONSC), aff'd 2011 ONCA 693.

72 *R v Morelli*, 2010 SCC 8 at paras 2-3, 105.

> 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.[73]

Personal computer searches are intrusive not only because of the sheer amount of information potentially accessible to authorities therein, but also because the digital nature of the information on a device distinguishes it from hard copy equivalents. Data stored on a computer may be created without conscious action or even knowledge of the user and may be recoverable even after the user tries to destroy it. The individual's control over personal information is reduced in digital data, and control over information is a key component of informational privacy.[74]

Not all computers evoke the same height of privacy concerns. There are all manner of already existing devices, ranging from fitness trackers to digital cameras and GPS modules to mobile phones, tablets, gaming systems, and smart watches. Each comes with its own potential and actual scope of available data. Not every laptop or tablet will contain the kind of vast treasure trove of personal footprints as the *Morelli* hard drive. Some phones may reveal even more extensive and intimate details than a desktop machine, whereas others may be used only as calling tools and not for any kind of on-device storage. Categories blend as technology moves forward—the computer is a phone, is a camera, is a watch. The majority of the SCC in *R v Fearon* made the important point that courts should avoid crafting different tests for the different capabilities of devices in some sort of categorical fixed list.[75]

Given the vast amount of information stored on digital tools in modern society, access to any kind of device may well trigger section 8 of the Charter. But every examination of a digital device does not inevitably result in an invasion of personal privacy or attract a high expectation of privacy. The nature and capability of the individual device, the use that is actually made of it, and the degree to which the state intrudes within the landscape of that potential will all influence the privacy assessment—including not just whether the threshold of engaging the section 8 protection is crossed, but also whether the remedy of exclusion of evidence under section 24(2) should be granted.

73 *Ibid* at paras 2-3.

74 *R v Vu*, 2013 SCC 60 at paras 24, 40-44.

75 *R v Fearon*, 2014 SCC 77 at para 52.

The degree of privacy intrusion matters under the section 24(2) analysis. The higher the privacy interest, the more intrusive the search; the more intrusive the search, the greater the impact on the accused's Charter-protected interests, and the more likely that the resulting evidence will be excluded. In *R v Adler*, the trial judge concluded that the warrantless search of the appellant's cellphone was not serious or impactful on the appellant because "[t]he privacy interests applied to the intimate secrets hidden in the subject's sock drawer is the same as the privacy interest in the intimate secrets hidden in his computer." The Court of Appeal for Ontario was quick to dismiss such reasoning, concluding that the trial judge "improperly minimized the privacy breach" given the well-established law in this area.[76]

The location of a device and nature of its use will be important considerations in the privacy analysis. For example:

- *A personal computer*, used at home, exclusively by one person, will undoubtedly garner a very high degree of privacy protection.[77] Even shared personal computers (e.g., between an individual and their spouse) attract section 8 protection, although the expectation of privacy may be diminished in certain circumstances.[78] Simply put, "[b]y choosing to share a computer with others, people do not relinquish their right to be protected from the unreasonable seizure of it."[79] Ownership is relevant, but not determinative, of the analysis.[80]

  It is readily inferred that a vast store of intimate details would be accessible on a personal computer, but all counsel should be wary of territorial assignments to digital data. The old spatial boundaries do not fit. Argument is better spent highlighting what the data will reveal, not where the box in which the information is stored was found.
- *A workplace computer* is likely to be lower on a privacy scale than an exclusively personal device, but, as noted above, categorical conclusions are dangerous. In *Cole*, the SCC affirmed a reasonable expectation of privacy in a workplace computer that is provided by the employer, monitored by the employer, and subject to use under explicit directions.[81] The user, Mr Cole, did not own or have exclusive control over data on his work computer, yet his expectation of privacy was objectively reasonable when considered in all of the circumstances. Factors such as habitual use and workplace culture, governing contracts, employer policies, systemic features and notifications regarding privacy, subjective belief and

76 *R v Adler*, 2020 ONCA 246 at paras 32-38.

77 *Morelli*, *supra* note 72 at para 105.

78 *R v Reeves*, 2018 SCC 56 at paras 36-39.

79 *Ibid* at para 37.

80 *Ibid* at para 39.

81 *Cole*, *supra* note 5 at para 3.

practice regarding monitoring, and multiple user access can all weigh in the mix and potentially impact the degree of privacy in a given situation.

- *A computer left in a repair shop* may also garner a reduced expectation of privacy.[82] A person who has knowingly turned over a device for maintenance should reasonably anticipate that another person will be reviewing or *seeing* at least some of the contents. But remember that privacy is a relational concept. Relinquishing control to a repair person does not extinguish one's privacy rights vis-à-vis the state. There may still be a reasonable expectation of privacy so as to trigger the application of section 8. However, the expectation of privacy would be diminished for the purposes of considering impact under section 24(2).
- *A computer carried across the border* takes on a unique characterization for the privacy inquiry. Travellers passing through international borders enjoy a reduced expectation of privacy.[83] In addition, separate statutes govern border control and related inspection. For instance, section 99(1) of the *Customs Act*[84] provides that an officer may "examine any goods that have been imported." Even still, to date, two Canadian appellate courts have held that to the extent that this provision authorizes digital devices to be searched without limits at the border, this interpretation violates section 8 of the Charter and cannot be justified under section 1.[85] In *R v Canfield*,[86] the Court of Appeal of Alberta stated that although "some of the information commonly stored on cell phones and other devices [e.g., receipts and other information relating to the value of imported goods] must be made available to border agents as part of the routine screening of passengers,"[87] the power to search digital devices cannot be limitless given the heightened privacy interests at stake. Accordingly, the Court granted a declaration of invalidity but suspended the declaration for one year.[88]

82 *R v Winchester*, 2010 ONSC 652 at paras 36, 73. But see *Cole*, *supra* note 5.

83 *R v Simmons*, 1988 CanLII 12 (SCC); *R v Jacques*, 1996 CanLII 174 at para 18 (SCC); *R v Monney*, 1999 CanLII 678 at para 42 (SCC); *R v Jones*, 2006 CanLII 28086 at paras 31-32 (ONCA); *R v Nagle*, 2012 BCCA 373.

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

85 *R v Canfield*, 2020 ABCA 383, leave to appeal to SCC denied, [2020] SCCA No 367 (QL); *R v Pike*, 2024 ONCA 608. But in British Columbia, see *R v Gibson*, 2017 BCPC 237; *R v Buss*, 2014 BCPC 16. For defence arguments against the ability of border officials to search the contents of digital devices, see Nader R Hasan & Stephen Aylward, "Cell Phone Searches at the Border: Privilege and the Portal Problem" (2017) 37:4 For the Defence 12.

86 *Canfield*, *ibid*.

87 *Ibid* at para 79.

88 *Ibid* at paras 111-15. The Court of Appeal of Alberta extended the initial one-year suspension period by six months (*R v Canfield*, 2021 ABCA 352) but declined to extend it beyond 18 months (*Her Majesty the Queen (Canada) v Canfield*, 2022 ABCA 145).

Similarly, in *R v Pike*, the Court of Appeal for Ontario denounced the legislation in clear terms:

> [I]t authorizes border officers to search some of the most private information imaginable on the lowest possible standard to justify a search, namely that in the border officers' own minds, they were sincerely trying to find evidence of border law violations. While sincerity is a good start, it is just not enough. Our *Charter* requires more because Canada's border control interests temper but do not eliminate or gut its protections.[89]

The Court held that border searches of digital devices should be governed by a reasonable suspicion standard. Unlike in *Canfield*, the *Pike* Court chose to read down the law, leaving the legislation intact: only the law's authorization to search digital devices at the border was unconstitutional, not its authorization to search other goods, which was not challenged. The Court suspended that declaration for six months.[90]

Note that despite the above declarations, both the *Canfield* and *Pike* courts declined to exclude the digital evidence seized at the border pursuant to section 24(2), largely due to border security officials' good faith reliance on their understanding of the scope of their search powers.[91] The Crown might argue that cases in the system before appellate court guidance was provided in this area should merit the same result, and that border security officials will need time to adapt. The defence, however, might counter this argument by trying to show, for example, additional or more serious Charter violations to support their argument for exclusion. And of course, the more time that passes between the *Canfield* and *Pike* decisions, the less likely the Crown's argument will find favour with the court.

Parliament is expected to legislate in this area. To date, Bill S-7, *An Act to Amend the Customs Act and Preclearance Act, 2016* has cleared the Senate and completed its first reading in the House of Commons.[92] Although provinces and territories other than Alberta and Ontario have not weighed in on this issue, border authorities across Canada should err on the side of strict constitutional compliance.

Mobile devices beyond the computer or smartphone can sometimes be overlooked. In all cases in which the police search or seize an item with a digital component, both Crown and defence counsel would be wise to consider whether it engages

89 *Pike*, *supra* note 85 at para 2.

90 *Ibid* at paras 103-8.

91 *Canfield*, *supra* note 85 at paras 185-86.

92 Bill S-7, *An Act to Amend the Customs Act and Preclearance Act, 2016*, 1st Sess, 44th Parl, 2021 (first reading 20 October 2022), online: <https://www.parl.ca/legisinfo/en/bill/44-1/s-7>.

a reasonable expectation of privacy. Non-traditional electronic devices defy categorical assessment, but in general, courts will likely assess the nature of the content, ownership, control, whether there are multiple users or people who have access, and the location of the device when obtained by police to consider whether or to what degree an individual can establish a reasonable expectation of privacy in the device. Consider, for example, the following types of "non-traditional" electronic devices:

- *Event Data Recorders (EDRs)*, also known as Airbag Control Modules, Sensing Diagnostic Modules, or Crash Data Retrievals, are airbag deployment devices in vehicles that record five seconds of vehicle data before a crash. They capture data regarding the speed, throttle, and braking of a vehicle before an airbag deployment or near-airbag-deployment event. Courts across Canada have recently considered the issue of whether EDRs attract a reasonable expectation of privacy. Appellate courts in British Columbia, Saskatchewan, and Ontario have held that they do not.[93] There is little difficulty in concluding that people have a *subjective* expectation of privacy in their EDR data. The focus of the debate has been on whether that expectation is objectively reasonable.

  In *R v Fedan*, *R v Major*, and *R v Attard*, three courts of appeal held that the lawful seizure of a vehicle pursuant to section 489(2) of the *Criminal Code* both (1) extinguishes a driver's territorial privacy interest in an EDR, and (2) eliminates any reasonable expectation of informational privacy in the EDR data.[94] Section 489(2)(c) authorizes the police to seize, without a warrant, "any thing that the officer believes on reasonable grounds … will afford evidence in respect of an offence." Of course, this analysis is premised on the *lawful* seizure of a vehicle pursuant to that section; this is the gateway to the lawful search and seizure of an EDR.[95] Prudent defence counsel may therefore challenge police grounds to seize a vehicle by arguing, for example, that the police did not have reasonable grounds to believe that a crime was committed at the time they seized the vehicle. In *Attard*, the Court of Appeal for Ontario held that the investigating officer had reasonable grounds to believe that the collision at issue was caused by excessive speed, leading him to conclude that he might be investigating a dangerous driving offence, and that the trial judge had erred in concluding the officer only had a reasonable suspicion.[96]

93 *R v Fedan*, 2016 BCCA 26, leave to appeal to SCC refused, 2016 CanLII 44776 (SCC); *R v Major*, 2022 SKCA 80, leave to appeal to SCC refused, 2023 CanLII 14940 (SCC); *Attard*, *supra* note 13.

94 *Fedan*, *ibid* at para 78; *Major*, *ibid* at para 70; *Attard*, *supra* note 13 at para 56.

95 *Fedan*, *ibid* at para 73; *Major*, *ibid* at para 63; *Attard*, *supra* note 13 at para 47.

96 *Attard*, *supra* note 13 at paras 20, 47-55.

- *Vehicle "dash cams"* typically have video, and sometimes audio, recording capabilities and can surveil the front, back, and inside of a vehicle. Some can connect to wi-fi or communicate with cellphones. At least one court has held that a dash cam attracts a reasonable expectation of privacy, although that expectation was greater regarding the recordings *inside* as opposed to *outside* the vehicle.[97] Officers obtaining a warrant to search a vehicle may therefore consider clearly and specifically seeking authorization to search and seize a dash cam.[98]

The reasonable expectation of privacy analysis is not fixed. As in any section 8 analysis, the nature of the information stored and accessible on a device will be relevant to assessing privacy in a normative fashion. The conclusions in the cases above are therefore not dispositive, and we can expect further litigation in this area as technology changes and evolves.

There is no limit to the types of evidence that might attract constitutional scrutiny if seized by the police. Consider, for example, devices like smart locks or door cameras; Fitbits and other devices that collect health information; or vehicle breaking records, which insurance companies routinely collect through cellphone applications to offer insurance incentives for safe driving. As technology evolves, more devices may be the subject of further litigation.

V. Expectation of Privacy in Online Activity

Online activity is, in many senses, public, and yet raises significant privacy concerns. In *Spencer*, the SCC considered the privacy implications of a police investigation into online activity. The Court found that the subscriber information obtained by police engaged section 8 of the Charter because of the information's *link to online activity*. The *Spencer* Court found that "subscriber information corresponding to specifically observed, anonymous Internet activity engages a high level of informational privacy."[99] Later, the Court again identified Internet subscriber information as private because it would "often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous."[100]

One principle guiding the finding of significant personal privacy in Internet activity is that of anonymity. We digitally travel far and wide and express or expose ourselves to any manner of intimate and revealing ideas, but often expect to do so unseen, unnamed, and unidentified. In defining privacy in the Internet context, the *Spencer*

97 *R v Rajaratnam*, 2024 ONSC 6894 at paras 28-31.

98 *Ibid* at paras 32-40.

99 *Spencer*, *supra* note 7 at para 51.

100 *Ibid* at para 66.

Court reviewed traditional concepts of secrecy in and control over information, establishing a third central component: anonymity. Cromwell J, for the Court, explained:

> There is also a third conception of informational privacy that is particularly important in the context of Internet usage. This is the understanding of privacy as anonymity. In my view, the concept of privacy potentially protected by s. 8 must include this understanding of privacy.[101]

The Court imported Doherty JA's analysis of privacy in online activity and related subscriber information from *Ward*,[102] another online child sexual abuse material case. In *Ward*, Doherty JA had identified anonymity as potentially requiring section 8 protection, depending on the totality of circumstances analysis. The *Spencer* Court similarly noted that anonymity is a factor that may take on greater or lesser significance in a given set of facts. Cromwell J cautioned:

> However, in my view, recognizing that there *may* be a privacy interest in anonymity depending on the circumstances falls short of recognizing any "right" to anonymity and does not threaten the effectiveness of law enforcement in relation to offences committed on the Internet.[103]

Of course, as with any privacy analysis, context-specific facts must be weighed in the balance. Online activity that includes user choice to publicly post identifiers may well be differently characterized at both the subjective and objective expectation of privacy determinations. The Crown is likely to argue the same with respect to online activity undertaken in circumstances of known surveillance or monitoring. The defence should be careful, however, to assess and respond to these arguments while bearing in mind the SCC's rejection of the US-style risk analysis (or assumption of risk doctrine, as it is sometimes called).[104] In other words, the defence response should be that it is not enough for the Crown to say that an Internet user assumed the risk of their privacy being invaded in engaging in a particular online activity. The ultimate question is a normative one—namely, *should* the law recognize a reasonable expectation of privacy vis-à-vis the state in the online activity in question?

One type of police activity that will push our thinking on this issue is the use of algorithmic technologies to collect and analyze data and metadata that are publicly available through open-source searches on the Internet. Facial recognition algorithms (e.g., Clearview AI) can be used to scrape images from the Internet, which are often

101 *Ibid* at para 41.

102 *Supra* note 46.

103 *Spencer*, *supra* note 7 at para 49 (emphasis in original).

104 *Cole*, *supra* note 5 at para 76; *R v Duarte*, [1990] 1 SCR 30 at 47-48, 1990 CanLII 150; *R v Wong*, [1990] 3 SCR 36 at 45, 1990 CanLII 56.

associated with identifiers such as social media usernames and profiles, and match them with the images on CCTV video from government cameras or private businesses. Pattern recognition algorithms can gather and analyze metadata, which may seem trivial as individual data points but which can paint incredibly detailed portraits of our private lives when aggregated. As the Officer of the Privacy Commissioner of Canada stated in their report on *Metadata and Privacy*, the traces we leave through our online activity can represent, "in aggregate form, a place holder for the intentions of humankind—a massive database of desires, needs, wants, and likes that can be discovered, subpoenaed, archived, tracked, and exploited to all sorts of ends."[105]

On one hand, the data and metadata being gathered and analyzed in these examples are all publicly available through open-source searches. The courts have not recognized a reasonable expectation of privacy in publicly available data. To do so, the Crown would argue, would be to go one step beyond *Spencer*, which dealt with subscriber information in the private possession of an ISP.

On the other hand, the defence may argue that the reasonable expectation of privacy analysis should develop to ensure some judicial oversight over these types of investigative activities, especially if privacy entails anonymity, as the SCC held in *Spencer*. In order to bring these activities within the rubric of the reasonable expectation of privacy analysis, the defence may argue that the subject of the search is not the collection of the individual pieces of data within the dataset, but rather the state action that searches for and obtains the patterns and inferences that are algorithmically drawn from the datasets. Post-*Bykovets*, focusing on the *use* of the information might carry purchase. In other words, the investigative technique and technology at issue enhance the intrusion of privacy. In this regard, the defence could analogize to the distinction between the use of a tracking device and human surveillance as recognized in *R v Wise*.[106]

VI. Expectation of Privacy in Sent Communications

In *Marakah*, the SCC addressed the thorny question of whether an individual has a reasonable expectation of privacy in sent communications obtained by the police from the recipient's device. So, for example, X sends Y a text. Police seize Y's phone and read the text. X is charged. The Crown seeks to use the text in a prosecution of X. X seeks to challenge the seizure or search of Y's phone in order to exclude the text from evidence. Does X have standing? Writing for the majority, McLachlin CJ answered

105 Office of the Privacy Commissioner of Canada, *Metadata and Privacy: A Technical and Legal Overview* (Gatineau, QC: OPC, 2014) at 4, online (pdf): <https://www.priv.gc.ca/media/1786/md_201410_e.pdf>.

106 1992 CanLII 125 (SCC). For a more robust analysis of how s 8 of the Charter might apply to data-collection algorithms, see Robertson & Presser, "Algorithmic Technology and Criminal Law in Canada" in Presser, Beatson & Chan, *Litigating Artificial Intelligence*, 2021/2022 ed (Toronto: Emond, 2021) 67 at 176-81.

that they did in the particular circumstances of that case, but declined to establish a categorical yes-or-no answer to the question of whether the sender maintains a reasonable expectation of privacy in sent communications.

Marakah involved SMS text messages between two parties—the accused, Mr Marakah, and his accomplice, Mr Winchester—about the sale of illegal firearms. McLachlin CJ began her analysis by examining the subject matter of the search. One view was that the subject matter of the search was the text message recipient's phone. In this way, *Marakah* would have been about the search of a device, and only the owner or user of that device would have had a reasonable expectation of privacy in its contents. McLachlin CJ rejected that view.[107] Instead, she described the "subject matter of the search" as "Mr. Marakah's 'electronic conversation' with Mr. Winchester."[108] She focused on text messages as a unique category of information and on the substance of the information sought rather than the physical place in which it was found.

Characterizing the subject matter of the search as an "electronic conversation" set the stage for the rest of McLachlin CJ's analysis. A conversation requires at least two parties. Each has an equal interest in the conversation, and each may have an equal expectation that it will remain private regardless of whose phone is searched by the police. The only question, then, is whether this expectation is reasonable.

The remainder of the factors in the "totality of the circumstances" test address this question of reasonableness. Two of these factors featured prominently in the Crown's submissions: the place of the search and the control exercised by the accused. These factors are critical in "territorial privacy" cases, where the focus is on the physical space in which items are found. However, because McLachlin CJ characterized the subject of the search as the electronic conversation between the sender and recipient, the application of the factors had to be adapted to the informational privacy context.

The place of the search, McLachlin CJ wrote, could be viewed as being the private electronic space that text messaging creates for the two parties to the conversation.[109] Meanwhile, control in the informational privacy context should be understood as the freedom of individuals to choose how, when, and to whom they disclose their information.[110] In the context of text messaging, individuals choose to disclose their private information to the recipient of the text message. This may necessitate a loss of control over the text message vis-à-vis the intended recipient, but that does not lead to the conclusion that the individual chose to give up their privacy rights vis-à-vis the rest of the world (and in particular the state).[111]

107 *Marakah*, *supra* note 10 at para 16.

108 *Ibid* at para 17.

109 *Ibid* at para 28.

110 *Ibid* at para 39.

111 *Ibid* at para 40.

The next factor to be examined was the nature of the information sought. Text messaging may be among the most private forms of communication. Individuals do not have to be in the same space to text message (and almost never are), and therefore do not run the risk of being seen together. Moreover, unlike phone conversations, text messaging allows individuals to communicate with others in complete privacy even while "in plain sight." As McLachlin CJ put it:

> A wife has no way of knowing that, when her husband appears to be catching up on emails, he is in fact conversing by text message with a paramour. A father does not know whom or what his daughter is texting at the dinner table. Electronic conversations can allow people to communicate details about their activities, their relationships, and even their identities that they would never reveal to the world at large, and to enjoy portable privacy in doing so.[112]

Based on the totality of the circumstances, McLachlin CJ concluded that individuals can retain a reasonable expectation of privacy in their text messages regardless of where the messages are discovered. Therefore, a sender of a text message may have standing to challenge an unconstitutional search of the recipient's device where that search revealed the sender's text messages.[113]

Writing on behalf of himself and Côté J, Moldaver J dissented. In his view, control was the most significant factor, and Mr Marakah gave up control over the text messages he sent to Mr Winchester when they were received on Mr Winchester's phone. At that point, Mr Winchester had exclusive control over the text messages on his device and had complete autonomy to disclose them to anyone, at any time, and for any purpose. This reality, in Moldaver J's view, was a compelling indicator that Mr Marakah did not have a reasonable expectation of privacy over the sent messages.[114] The majority, however, rejected this argument as taking too narrow a view of how control factors into the section 8 analysis in informational privacy cases.[115]

How far does the holding in *Marakah* extend? On one hand, McLachlin CJ explained that "text messaging" in the *Marakah* sense should be understood to include not only SMS messages but "various other person-to-person electronic communications tools, such as Apple iMessage, Google Hangouts, and BlackBerry Messenger."[116] On the other hand, she clarified that not every communication

112 *Ibid* at para 36.

113 For a deeper analysis of *Marakah*, see Gerald Chan, "Text Message Privacy: Who Else Is Reading This?" (2019) 88 SCLR: Osgoode's Annual Constitutional Cases Conference 69, online: <https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1361&context=sclr>.

114 *Marakah*, *supra* note 10 at paras 144-46, Moldaver J in dissent.

115 *Ibid* at paras 44-45.

116 *Ibid* at para 18.

occurring through an electronic medium will attract a reasonable expectation of privacy, emphasizing that *Marakah* did not concern "messages posted on social media, conversations occurring in crowded Internet chat rooms, or comments posted on online message boards."[117]

The SCC again considered the issue of reasonable expectation of privacy in text message communications in *R v Campbell*.[118] There, the police arrested a suspected drug dealer and seized his cellphone incident to arrest. Several messages suggestive of an ongoing drug transaction appeared on the cellphone's home screen. The police impersonated the dealer and continued to communicate with the message sender to complete the drug delivery. Mr Campbell attended the agreed-upon meetup location with the drugs, and the police arrested him. He testified that he was using a borrowed phone to complete the drug delivery.

One of the issues at trial was whether Mr Campbell, the message sender, had a reasonable expectation of privacy in his conversation on the dealer's phone. The SCC held that he did. Their analysis focused on three factors: the private subject matter, the intrusiveness of the police investigation, and control. The Court re-emphasized the intensely private nature of text messaging; a form of communication in which reasonable people expect "the utmost privacy" given "the potential or tendency to reveal deeply personal and biographical information about the participants."[119] The police investigative technique was also especially intrusive; they essentially "hijacked" the identity of one of the conversation participants, inserting themselves into a private conversation that was already underway.[120] Finally, the Court held that the phone being borrowed did not undercut Mr Campbell's reasonable expectation of privacy because he had a prior relationship with the phone owner, and because control is not determinative of standing. In other words, shared control may diminish, but not eliminate, a reasonable expectation of privacy.[121]

Contrast *Campbell* with the Court of Appeal for Ontario's decision in *R v Knelsen*.[122] There, the complainant voluntarily provided electronic communications between herself and the appellant to the police in furtherance of a sexual assault and child luring investigation. The Court held that the appellant *did not* have an objectively reasonable expectation of privacy in the messages. In doing so, the Court emphasized what the police knew based on their interview with the complainant *before* she gave them the messages: that he was an adult and she was 15 years old, and that the appellant knew that; that they were practically strangers, having only met

117 *Ibid* at para 55.

118 *Supra* note 11.

119 *Ibid* at paras 55-61.

120 *Ibid* at paras 62-63.

121 *Ibid* at paras 64-68.

122 2024 ONCA 501, leave to appeal to SCC dismissed, 2025 CanLII 20251 (SCC).

once; and that they were communicating for the purpose of arranging to meet for sex. Moreover, the appellant ought to have expected that the complainant would have shared their messages, including potentially with law enforcement, given her age and the circumstances. Citing the SCC's decision in *R v Mills*,[123] the Court held that the appellant's subjective expectation of privacy was therefore not objectively reasonable considering the totality of the circumstances and the societal goals of protecting children from sexual exploitation.[124]

Similarly, in *R v PM*,[125] the Court of Appeal for Ontario held there was no reasonable expectation of privacy in text messages the appellant had sent to his ten-year-old niece. Given the complainant's age, it would have been obvious to a reasonable person that her parents would exercise control over her phone, including reviewing its contents. Moreover, relying on *Knelsen*, the Court found that any subjective expectation of privacy was not reasonable in light of the societal interest in protecting children from sexual offences facilitated by electronic communication.

Several courts have considered whether *Mills* created a "*Marakah* exception" for communications forming the subject matter of an offence. This issue has not been definitively resolved.

Mills involved an undercover online sting operation where the police posed as an underage girl for the purpose of investigating child luring. The accused communicated with the undercover officer and later argued that the police had infringed his section 8 rights by intercepting those communications without prior judicial authorization. A majority of the SCC held that there was no section 8 violation, but the four sets of concurring reasons have left courts and litigants unclear about its precise scope. That said, the thrust of the *Mills* decision was that a person does not have an objectively reasonable expectation of privacy when communicating with a child online that they do not know, particularly when the police know that to be the case because they created the underage child.[126]

In the Court of Appeal for Ontario's decision in *Campbell*, before it reached the SCC, Trotter JA suggested that *Mills* created an exception for circumstances where "the electronic communications themselves constitute a crime against the recipient,"[127] the result being that there is no objectively reasonable expectation of privacy where the evidence seized is the means of committing the offence charged. The *Knelsen* Court relied on *Campbell* in also concluding that because the messages at issue were sent in furtherance of committing the offences of sexual assault and child

123 2019 SCC 22.

124 *Knelsen*, *supra* note 122 at paras 57-60.

125 2025 ONCA 208.

126 *Mills*, *supra* note 123 at para 30, Brown J.

127 *R v Campbell*, 2022 ONCA 666 at paras 62, 73. See also *R v Lambert*, 2023 ONCA 689 at para 60.

luring, the appellant had no reasonable expectation of privacy therein.[128] The Court of Appeal for Ontario again reached the same conclusion in *R v Gauthier*, this time regarding a threatening voicemail: because the appellant's voicemail was the means of committing the offence of criminal harassment and harassing communications—that is, the communications themselves constituted a crime—the appellant did not have a reasonable expectation of privacy in that evidence.[129]

In *Campbell* (SCC), the Court left the issue of whether a "*Marakah* exception" exists to another day. It stated that, given the varying sets of reasons from the SCC in *Mills*, there was no majority decision. For that reason,

> *Marakah* remains the governing authority on when a text message conversation attracts a reasonable expectation of privacy under s. 8. It is thus not necessary to decide whether *Mills* is properly characterized as creating an "exception" to *Marakah* or as departing from the content-neutral approach to s. 8 of the *Charter*.[130]

This area, therefore, remains ripe for litigation. Defence counsel might argue that focusing on the subject matter of the evidence seized is inconsistent with the content-neutral approach to section 8 jurisprudence that the SCC has espoused for decades.[131] Crown counsel, however, might argue that there are compelling public policy reasons for considering broader societal concerns when setting the boundaries of section 8, a competing principle appellate courts have also broadly recognized.[132]

VII. Summary

Recent SCC jurisprudence demonstrates several trends in the area of digital privacy. First, the Court appears increasingly willing to find a reasonable expectation of privacy in digital spaces (e.g., *Marakah*, *Campbell*, *Bykovets*). Second, there has been a focus on the *potential* to reveal personal, biographical information (e.g., *Bykovets*, *Campbell*). And finally, the Court has been increasingly willing to find a section 8 violation in circumstances involving evidence being given to the police with the consent of a third party (e.g., *Reeves*, *Bykovets*), although it has yet to definitively resolve the issue of whether section 8 is engaged in cases involving the voluntary provision of evidence, such as text messages, to the police.[133]

128 *Campbell*, *ibid* at paras 61-65.

129 *R v Gauthier*, 2024 ONCA 621 at paras 42-44.

130 *Campbell* (SCC), *supra* note 11 at para 78.

131 See Martin J's forceful dissent in *Mills*, *supra* note 123 at para 110. See also e.g. Chelsey Buggie, "Talking to Strangers: A Critical Analysis of the Supreme Court of Canada's Decision in R v Mills" (2021) 44:6 Man LJ 108.

132 See e.g. the discussion in *R v Singh*, 2024 ONCA 66 at para 63.

133 *Reeves*, *supra* note 78 at para 46. See also *Knelsen*, *supra* note 122 at para 47 and *PM*, *supra* note 125 at paras 52-57.

If there is one clear conclusion to draw from the varied case law on reasonable expectations of privacy in a digital era, it is that there are no clear fixed lines. Privacy is normative. Values change. In the area of digital information sharing and storage, values and practices change daily. For litigators, it is worth spending the time to work through the complex analysis of what constitutes a reasonable expectation of privacy. For Crown counsel, it is the threshold issue that can shut down challenges from the outset. For defence counsel, everything is up for grabs.

Categorical approaches are not fruitful. Each case will turn on the totality of circumstances, including spatial context, ownership, and access to devices, as well as the fair characterization of information both sought and obtained regarding the scale of intimacy and invasiveness.