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.

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 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 need 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, 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 need to understand the first principles of privacy to effectively argue about appropriate extensions of those principles and the attendant rights and state obligations in digital contexts.

II. Defining Privacy

Privacy may be physical, territorial, or informational. Digital evidence most commonly engages concerns over informational privacy. 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. A bedroom tablet may also 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 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.

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

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

Traditional privacy analysis focused largely on the tangible factors of control and access to locations where evidence was seized. In *R v Edwards*,[3] the Supreme Court of Canada (SCC) set out a flexible framework with key questions to ask in assessing privacy interests.[4] 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.[5]

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.[6]

Several modifications of the totality of circumstances test have been articulated to organize analysis in a given fact scenario. For example, in *R v Patrick*,[7] Binnie J listed factors similar to those in *Edwards* but geared toward addressing situations where territorial and information privacy overlap. *Patrick* dealt with garbage bags put out for collection and retrieved by police. *R v Spencer*[8] dealt 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; and (4) whether this subjective expectation of privacy was objectively reasonable given the totality of the circumstances.[9] None of these tests are inconsistent; they are articulations of the same overarching concerns grouped differently as suited to a particular inquiry. Again, argument on what data were seized, not on where the machine sat at seizure or during use, is the best focus.

3 [1996] 1 SCR 128, 1996 CanLII 255.

4 *Ibid* at para 45.

5 *Ibid*.

6 See e.g. *R v Plant*, [1993] 3 SCR 281, 1993 CanLII 70 at para 45; *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.

7 *Supra* note 6 at para 27.

8 2014 SCC 43.

9 *Ibid* at para 18.

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."[10] 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.[11] Thus, section 8 of the Charter did not apply to the access that police gained to a computer terminal set up by the utility to allow police to look up the appellant's electrical consumption records.

In *R v Gomboc*,[12] however, information of a similar nature had a different hue.[13] 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., cannabis grow operation).

The strength of the inference supported by the information is critical.[14] 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*, in arguing that data reveal more about the target than a simply 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.

10 *Plant*, *supra* note 6 at para 20.

11 *Ibid*.

12 2010 SCC 55.

13 *Ibid* at para 38, Deschamps J; para 81, Abella J; and paras 128-32, McLachlin CJ and Fish J, dissenting.

14 See discussion of *Gomboc* by the Court in *Spencer*, *supra* note 8 at para 30.

In *R v Orlandis-Habsburgo*,[15] the Court held that the accused had a reasonable expectation of privacy in his energy consumption data. In that case, the police obtained the data from the electrical utility provider. The data showed the accused's energy consumption levels on an hourly basis, which provided a strong inference that a specific activity—a cannabis grow-op—was being conducted within the residence. This, the Court held, supported the finding that the accused had a reasonable expectation of privacy because activities conducted within one's home "fall at the centre of the zone of personal privacy."[16]

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).[17] The importance of defining the subject matter of the search was reinforced in *Spencer*.[18] There, the SCC considered whether individuals have a reasonable expectation of privacy in their 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 the IP address (the individual's online activities).[19] 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."[20] 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.[21] 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.

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

15 2017 ONCA 649.

16 *Ibid* at paras 75-76.

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

18 *Supra* note 8.

19 *Ibid* at para 24.

20 *Ibid* at para 66.

21 *Ibid*.

establishing a subjective expectation of privacy is relatively modest.[22] 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.[23] 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.[24] 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.[25]

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.[26] 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 privacy of 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. 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. 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."[27] In the public spaces of online activity, the line is no longer as clear.[28] Digital information is constantly shared with some sections of the public, but strictly guarded by its owner as against others. There is a distinct and growing tension between the competing desires for privacy and publicity.

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

23 *Ibid* at para 21.

24 *Ibid* at para 9.

25 *Ibid* at para 22.

26 *Spencer*, *supra* note 8 at para 18; *Tessling*, *supra* note 6 at para 42; *Patrick*, *supra* note 6 at para 14.

27 *Tessling*, *supra* note 6 at para 40.

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

The SCC elaborated on a modern legal conception of privacy in *Spencer*, defining informational privacy as comprised of three elements: secrecy, control, and anonymity.[29] 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 Ontario Court of Appeal decision in *R v Ward*.[30] 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.[31]

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.[32]

The SCC considered the factor of control in the cases of *Cole*[33] and *R v Marakah*.[34] *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

29 *Supra* note 8 at para 38.

30 2012 ONCA 660.

31 *Ibid* at para 71; see also paras 72-74.

32 *Spencer*, *supra* note 8 at para 49 (emphasis in original).

33 *Supra* note 6.

34 2017 SCC 59.

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."[35] 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.[36] 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 privacy when they create the risk that their information will fall into the hands of the state).[37] 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.[38]

Ultimately, the reasonable expectation of privacy analysis requires an examination of the totality of circumstances. While this approach facilitates flexible and contextual decision-making, questions remain as to how police will be able to translate such nuanced analysis into front-line decisions about the scope of their powers.

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 reveal when combined with other pieces of state evidence. Some trends are discernable in the manner in which courts approach different types of digital evidence.

III. Expectation of Privacy in Subscriber Information

Subscriber information is basic information about a person who enters a contract for telecommunications or other services. In the context of digital evidence, subscriber information usually includes the customer name, municipal address, billing information, and account details obtained from a telecommunications service provider. The kind of service at issue and the basis of the police request for information will

35 *Ibid* at para 38; *Cole*, *supra* note 6 at paras 54, 58.

36 *Marakah*, *supra* note 34 at para 39.

37 *Ibid* at para 41.

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

influence whether and what kind of judicial authorization is required for the state to access subscriber information.

In *Spencer*,[39] 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 pornography 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 pornography transmission to a particular suspect, police requested basic subscriber information from the ISP associated with the IP at the relevant time period. There was no judicial pre-authorization. The ISP responded to the request and provided a name, municipal address, and basic account details. Police obtained a search warrant for the address, where they located a computer belonging to Matthew Spencer (not the service subscriber) that contained child pornography.

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*,[40] 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."[41] 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

39 *Supra* note 8.

40 2020 SCC 11.

41 *Ibid* at para 36.

always require fact-specific analysis of the totality of circumstances. There remains a lot up for grabs in this context.

In the post-*Spencer* case of *HMQ v TELUS Communications Co*,[42] the Ontario Superior Court held that not all customer name and address information attracts a reasonable expectation of privacy.[43] In *TELUS*, police had obtained a transmission data recorder warrant (TDRW) under section 492.2 of the *Criminal Code*.[44] 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.[45] 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.[46]

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.[47] The courts have long held that there is a reasonable expectation of privacy in this information, including in *R v Rogers Communications*.[48]

The Ontario Superior Court of Justice decision in *TELUS* concluded that there was no reasonable expectation of privacy in basic telephone subscriber information.

42 2015 ONSC 3964 [*TELUS*].

43 *Ibid* at para 24.

44 RSC 1985, c C-46; 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.

45 *Supra* note 8 at para 40.

46 *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.

47 *TELUS*, *supra* note 42 at para 37.

48 2016 ONSC 70 at para 31 (Sup Ct J). See also *R v MacInnis*, [2007] OJ No 2930 (QL) (Sup Ct J); *R v Mahmood*, 2008 CanLII 51774, [2008] OJ No 3922 (QL) (Sup Ct J), aff'd 2011 ONCA 693.

Unlike online activity, telephone conduct has historically been more limited in scope and not anonymous, given the public listing of most numbers and addresses in virtual, if not paper, phonebooks. However, 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 will continue or begin to attract a reasonable expectation of privacy.

Defence counsel seeking to establish a reasonable expectation of privacy in the 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. Social science literature, polls or surveys on the widespread use of new technological tools or apps, and privacy commission reports 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.

IV. Expectation of Privacy in a Computer or Device

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*[49] to be the most intrusive state search imaginable.[50] In the oft-quoted introduction to the majority decision in *Morelli*, Fish J described the scale of privacy interest in a home computer search:

> 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.[51]

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.

49 2010 SCC 8.

50 *Ibid* at paras 2-3, 105.

51 *Ibid* at paras 2-3.

Data stored on a computer may be created without conscious action or even knowledge of the user and may remain, in recoverable form, 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 to informational privacy.[52]

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*[53] made the important point that courts should avoid crafting different tests for the different capabilities of devices in some sort of categorical fixed list.[54]

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 a vast 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. 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.

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.[55] In addition, while the sharing of a personal computer (e.g., between an individual and their spouse) may result in a diminished expectation of privacy, the expectation of privacy will nonetheless be sufficiently reasonable to attract section 8 protection.[56]

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

53 2014 SCC 77.

54 *Ibid* at para 52.

55 *Morelli*, *supra* note 49 at para 105.

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

  - 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 don't fit. Argument is better spent on highlighting what the data will reveal, not where the box in which the information was 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 cautions.[57] 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 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.[58] 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 different characterization for the privacy inquiry. Travellers passing through international borders enjoy a reduced expectation of privacy.[59] In addition, separate statutes govern border control and related inspection. For instance, section 99(1) of the *Customs Act*[60] provides that an officer may "examine any goods that have been imported." Several lower courts have held that this provision, which enables "goods" to be searched without limits at the border, applies to the search of digital devices.[61]

57 *Supra* note 6 at para 3.

58 *R v Winchester*, 2010 ONSC 652 at para 36, 73. But see *Cole*, *supra* note 6.

59 *R v Simmons*, [1988] 2 SCR 495, 1988 CanLII 12; *R v Jacques*, [1996] 3 SCR 312, 1996 CanLII 174 at para 18; *R v Monney*, [1999] 1 SCR 652, 1999 CanLII 678 at para 42; *R v Jones*, 2006 CanLII 28086, 81 OR (3d) 481 at paras 31-32 (CA); *R v Nagle*, 2012 BCCA 373.

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

61 *R v Saikaley*, 2012 ONSC 6794 at para 82, appeal allowed in part on other grounds, 2017 ONCA 374; *R v Gibson*, 2017 BCPC 237 at para 201; *R v Buss*, 2014 BCPC 16 at paras 25-32; *R v Moroz*, 2012 ONSC 5642 at para 20; *R v Leask*, 2008 ONCJ 25 at para 18; and other cases cited in *R v Canfield*, 2020 ABCA 383 at para 69, leave to appeal denied [2020] SCCA No 367 (QL).

In *R v Canfield*,[62] however, the Alberta Court of Appeal held that section 99(1) (so interpreted) violates section 8 of the Charter and that this violation cannot be justified under section 1. While "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,"[63] 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.[64]

Mobile devices beyond the computer or smartphone again 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.

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 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."[65] 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."[66]

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* Court reviewed traditional concepts of secrecy in and control over information,

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.

62 *Supra* note 61.

63 *Ibid* at para 79.

64 *Ibid* at paras 111-15.

65 *Supra* note 8 at para 51.

66 *Ibid* at para 66.

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.[67]

The Court imported Doherty JA's analysis of privacy in online activity and related subscriber information from *Ward*,[68] another online child pornography 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.[69]

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).[70] 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 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

67 *Ibid* at para 41.

68 *Supra* note 30.

69 *Spencer*, *supra* note 8 at para 49 (emphasis in original).

70 *Cole*, *supra* note 6 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."[71]

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. 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*.[72]

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 that they did in the particular circumstances of that case, but declined to

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

72 [1992] 1 SCR 527, 1992 CanLII 125. 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* (Toronto: Emond, 2021) ch 3 at 176-81.

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.[73] Instead, she described the "subject matter of the search" as "Mr. Marakah's 'electronic conversation' with Mr. Winchester."[74] 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.[75] 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.[76] 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).[77]

73 *Marakah*, *supra* note 34 at para 16.

74 *Ibid* at para 17.

75 *Ibid* at para 28.

76 *Ibid* at para 39.

77 *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.[78]

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.[79]

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.[80] 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.[81]

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."[82] On the other hand, she clarified that not every communication

78 *Ibid* at para 36.

79 For a deeper analysis of *Marakah,* see Chan & Gerald, "Text Message Privacy: Who Else Is Reading This?" (2019) 88 SCLR: Osgoode's Annual Constitutional Cases Conference (2d) 69, online: <https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1361&context=sclr>.

80 *Marakah*, *supra* note 34 at paras 144-46, Moldaver J in dissent.

81 *Ibid* at paras 44-45.

82 *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."[83] The distinction appears to be that between person-to-person communications and communications to a broader audience. But as we discuss in more detail in Chapter 4, even person-to-person communications do not always attract a reasonable expectation of privacy based on how courts have since interpreted *Marakah*. The analysis remains one that demands consideration of the totality of the circumstances, an approach that ensures flexibility and contextual decision-making, if not predictability.

VII. Summary

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 sought and obtained regarding the scale of intimacy and invasiveness.

83 *Ibid* at para 55.